Micronet®
Faster and Easier Networks

User’s Manual

48-Port Gigabit Web Smart Switch

Model No.: SP6148WS

http://www.micronet.info

Contents

1. INTRODUCTION 1

1.1 PACKAGE CONTENTS 1
1.2 KEY FEATURES 1
1.3 FRONT PANEL VIEW 2
1.3.1 LED Indicators 2
1.4 REAR PANEL VIEW 3

2. INSTALLATION 4

2.1 HARDWARE AND CABLE INSTALLATION 4
2.1.1 Installing Optional SFP Fiber Transceiver 4
2.1.2 Connecting the SFP Module to the Chassis 4
2.1.3 TP Port and Cable Installation 4
2.1.4 Powering On 5
2.1.5 Installing Chassis to a 19-Inch Wiring Closet Rail 5
2.1.6 Cabling Requirements 5
2.2 CONFIGURING MANAGEMENT AGENT 6
2.2.1 IP Address Configuration 6

3. WEB-BASED USER INTERFACE 7

3.1 SYSTEM CONFIGURATION 7
3.1.1 System Information 7
3.1.2 IP Configuration 9
3.1.3 Time Configuration 9
3.1.4 Account Configuration 11
3.2 PORT CONFIGURATION 13
3.2.1 Port Status 13
3.2.2 Simple Counter 14
3.2.3 Detail Counter 15
3.3 STORM 18
3.3.1 Storm Control 18
3.4 MIRROR 20
3.4.1 Mirror Setting 20
3.5 FILTER 21
3.5.1 Filter Setting 21
3.6 QOS 22
3.6.1 Priority Configuration 22
3.6.2 IP Layer Priority State Setting 22
3.6.3 Differentiated Service Code Point (DSCP) 23
3.6.4 Port Priority Setting 23
3.6.5 Shaper Queue 24
3.6.6 ACL Priority Override 24

3.6.7 Policer Configuration....25
3.6.8 Shaper Setting....26
3.6.9 Flow....27
3.6.10 IP Flow ID Ignore Setting....28
3.6.11 IP Flow ID Configuration....28
3.6.12 Static Forwarding MAC....29
3.6.13 Policer Flow ID Table....30
3.6.14 Mark Priority....31
3.6.15 Mark-enable CoS/DSCP....32
3.6.16 ACL....32
3.6.17 ACL/VLAN Mapping....33
3.6.18 ACL Rule....33
3.6.19 ACL Rule Setting....34
3.6.20 ACL QoS Load....36
3.6.21 User Defined....36
3.7 SNMP....37
3.7.1 SNMP Configuration....37
3.8 LINK AGGREGATION....39
3.8.1 Aggregation Configuration....39
3.9 ALARM CONFIGURATION....40
3.9.1 Trap Events Configuration....40
3.9.2 Email/SMS Configuration....40
3.10 CONFIGURATION....42
3.10.1 Save Start....42
3.10.2 Restore Default....42
3.10.3 Restore User....42
3.11 DIAGNOSTICS....43
3.11.1 Diagnostics....43
3.11.2 Loopback Test....43
3.11.3 Ping Test....44
3.12 TFTP....45
3.12.1 TFTP Server....45
3.13 LOG....46
3.13.1 Log Data....46
3.14 FIRMWARE....47
3.14.1 Firmware Upgrade....47
3.15 MAX. PACKET LENGTH....48
3.15.1 Maximum Packet Length Configuration....48
3.15.2 Static Forwarding MAC....48
3.15.3 Static Filtering MAC....49
3.16 VLAN....50
3.16.1 VLAN Mode....50
3.16.2 Tag-based VLAN....50
3.16.3 Port-based VLAN....52

3.16.4 Port Protocol Setting 54
3.16.5 Port VID 55
3.17 REBOOT 56
3.17.1 Reboot the System 56
3.18 LOGOUT 57

4. TROUBLESHOOTING 58

5. TECHNICAL SPECIFICATION 59

1. Introduction

Micronet SP6148WS 48-port Gigabit Web Smart Switch delivers truly non-blocking and wire-speed Gigabit performance for enterprises and service providers that demand high-port density applications. Moreover, it brings advanced features, including tag-based VLAN, port trunk, L2/L3/L4 traffic prioritization, bandwidth control, and ACL, to optimize the network.

In the switch, Port 45 - 48 include two types of media: TP and SFP Fiber (LC, BiDi-LC…). These ports support 10/100/1000Mbps TP or 1000Mbps SFP Fiber with auto-detected function. 1000Mbps SFP Fiber transceiver is used for high-speed connection expansion.

1.1 Package Contents

- Gigabit Web Smart Switch
- Mounting Accessory (for 19” Rack Shelf)
- Quick Installation Guide
- CD-ROM with User Manual
- AC Power Cord

1.2 Key Features

- IEEE802.3 10Base-T, IEEE802.3u 100Base-TX, IEEE802.3ab 1000Base-T, and IEEE802.3z 1000Base-LX/SX standards.
- 48 x 10/100/1000M RJ-45 ports and 4 x shared SFP slots
- 48Gbps non-blocking switching capability
- Wire-speed performance at jumbo packet size of 16K byte
- Head of Line (HOL) blocking prevention
- IEEE802.1q tag-based VLAN, 256 VLAN groups
- Traffic optimization using various class of service option: per-port, L2 priority (802.1p), L3 priority (TOS or DSCP), L4 priority (TCP/UDP service number), and IPv6 traffic class
- 4 hardware priority queues
- Enhanced traffic rule and security by L2/L3/L4 ACL (Access Control List)
- Broadcast and multicast storm control
- Ingress and egress per port bandwidth control
- Port trunk with flexible load distribution and failover function
- SNMP trap, E-mail and SMS alarm for any connectivity events

1.3 Front Panel View

The switch provides 44 Port 10/100/1000Mbps TP and 4 Port Gigabit TP/SFP Fiber. LED lights for Power/CPU are placed on the left hand side of the front panel. Port status indication LEDs are located on the top right hand side of each port. For details on LED indications, refer to section 1.3.1 LED Indicators.

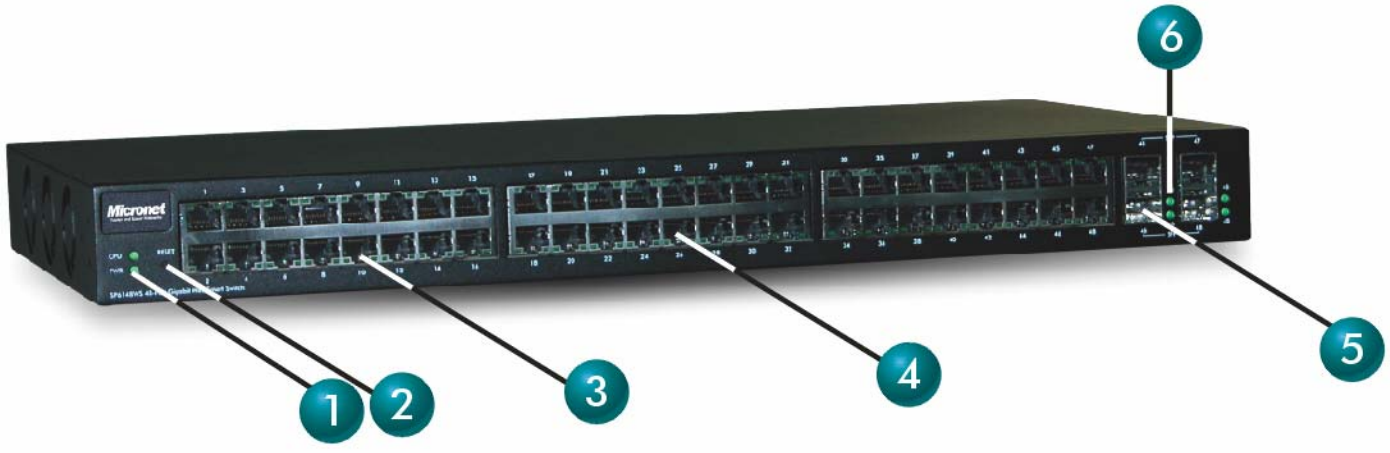


Fig. 1.1 Front Panel View

1. Power/CPU Indication
2. Reset Button
3. TP Port LED
4. Gigabit Ethernet Port
5. SFP Fiber Port
6. Fiber Port LED

1.3.1 LED Indicators

LED	Status	Operation
System LED		
POWER	On/Green	Power is on
CPU	Blink/Green	Switch is working properly
	Off	CPU fails or initializes
10/100/1000Ethernet TP Port (1 to 48 port)		
LINK/ACT	On/Green	Link with remote device is good
	Blink/Green	Traffic is present
	Off	Link is off or bad connection
10/100/1000M	On/Green	1000M link is detected
	Blink/Green	100M link is detected
	Off	10M or no link is detected
1000SX/LX Gigabit Fiber Port (45 - 48 port)		
SFP (LINK/ACT)	On/Green	Link with remote device is good
	Blink/Green	Traffic is present

	Off	Link is off or bad connection

1.4 Rear Panel View

Fig. 1.2 Rear Panel View

2. Installation

These three sections provide users a quick start on installation.

- Hardware and Cable Installation
- Management Station Installation
- Software Booting and Configuration

2.1 Hardware and Cable Installation

Prior to installation, please wear grounding device to prevent electrostatic discharge on equipment.

2.1.1 Installing Optional SFP Fiber Transceiver

(Note: Skip this section if no modules are installed.)

Attach the SFP fiber transceiver according to the figure below. Supported SFP transceivers include RubyTech Corporation, Avago Technologies and Finisa Corporation.

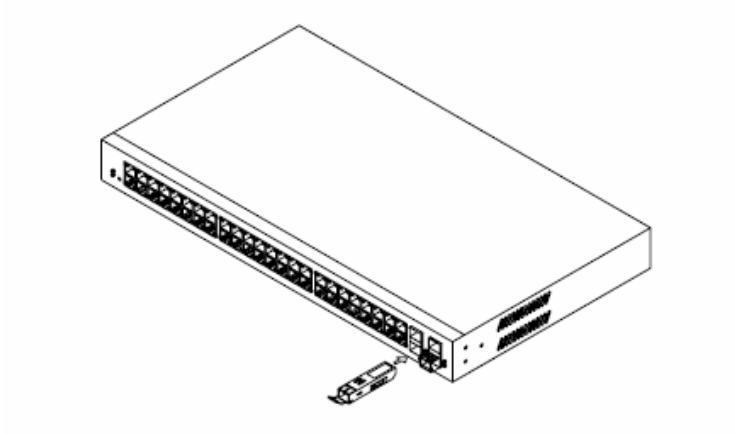


Fig. 2.1 Installing SFP Fiber Transceiver

2.1.2 Connecting the SFP Module to the Chassis

The SFP modules can be plugged or unplugged while the device is still powering on.

1. Verify the SFP module is the right model and conforms to the chassis.
2. Slide the module carefully along the slot and ensure it is properly seated against the slot socket/connector.
3. Attach the media cable for network connection.
4. Repeat steps above for each module to be installed.

2.1.3 TP Port and Cable Installation

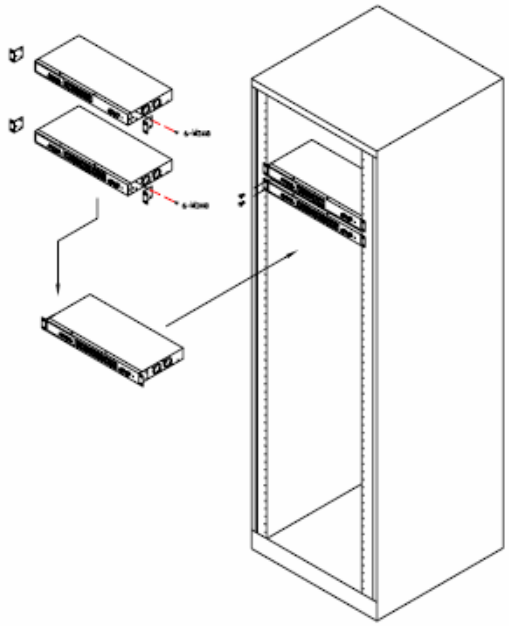
1. TP ports support MDI/MDI-X auto-crossover, therefore both straight-through and crossed-over can be used.
2. Cat.5 grade RJ-45 TP cable is to be used to connect to a TP port and the other end is connected to a network-aware device.

3. Repeat steps above for each TP port to be installed.

2.1.4 Powering On

The switch's power adapter supports 100-240 VAC and 50-60 Hz. The power supply will automatically convert the local AC power source to DC power. The power socket can be located on the right hand side of the rear panel. For further information, refer to figure 1.2 Rear Panel View.

2.1.5 Installing Chassis to a 19-Inch Wiring Closet Rail



1. Allow space for air ventilation on both sides of the chassis.
2. Wear grounding device to prevent electrostatic discharge on equipment.
3. Attach the mounting accessory to the front side of the switch.
4. Gently place the chassis into the 19-inch wiring closet rail and adjust it to the correct position. Tighten the chassis by tightening the screws.

2.1.6 Cabling Requirements

The table below is the cable requirements for ensuring optimal network performance.

Connection Type	Cable Requirements	Maximum Length
Fast Ethernet TP	Cat.5	100 meters
Gigabit Ethernet TP	Cat. 5 (recommend Cat. 5e)	100 meters

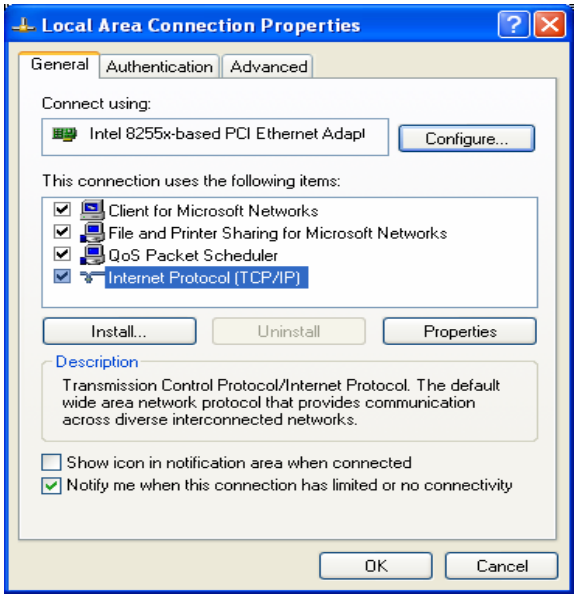
Table 2.1 Cable Requirements

2.2 Configuring Management Agent

2.2.1 IP Address Configuration

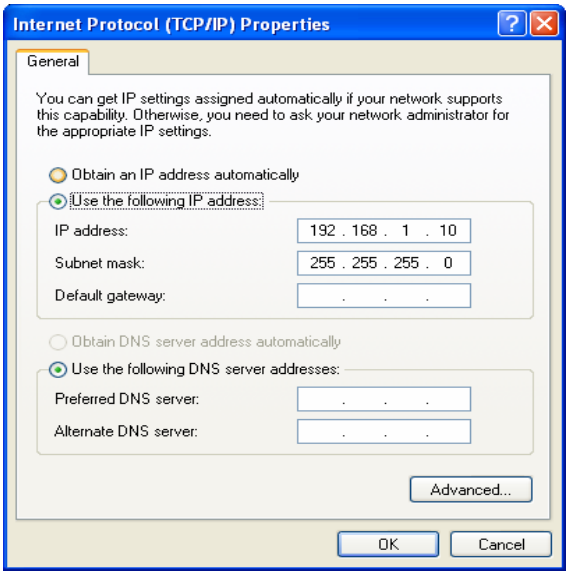
PC/Notebook must belong in the same IP range and subnet. Follow the steps below to configure IP settings for LAN PC.

Step 1. In the control panel, double click on Network Connections. Double click on the local area connection (e.g. LAN). The following screen will appear.



Step 2. Select 'Internet Protocol (TCP/IP)', and then click on the 'Properties' button. The screen will appear to allow entry of TCP/IP settings.

Step 3. Select 'Use the following IP Address' button and then enter the IP address and subnet mask. Ensure the IP address and subnet mask are on the same subnet as the switch. Click on 'OK' button to save the setting.

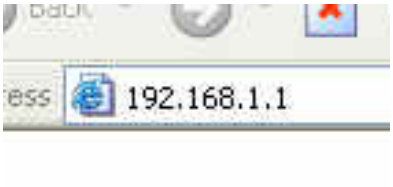

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 1 . 10
Subnet mask: 255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Default Values

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
Password	admin

3. Web-based User Interface

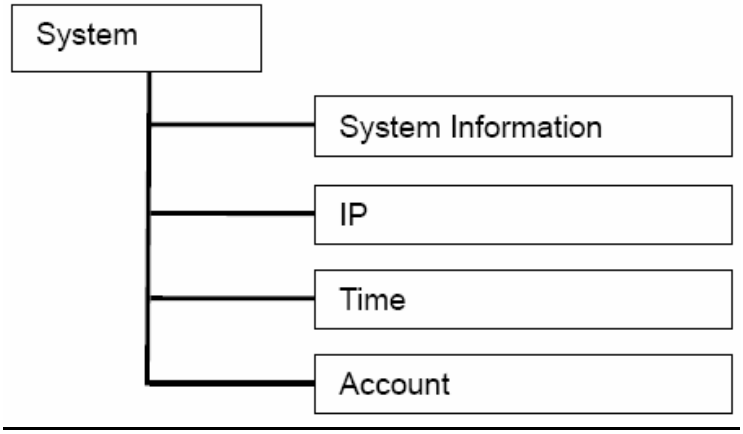
SP6148WS is embedded with http sever and provides a series of web pages, which display the configuration and status of the system. After configuration of IP, the management interface can be access by entering the IP address of the switch into the browser.



The system will prompt the user to enter password for authentication purpose. Once password is correctly entered, a web page will appear for configuration and management. On the left hand side of the browser will contain a menu tree with list of functions. Menu is in hierarchical structure and opening the menu will display a sub-menu.

3.1 System Configuration

System configuration is divided into four components and will be explain in details in the upcoming sections.



3.1.1 System Information

This function will allow users to view system information.

Parameter	Description
Model Name	The model name of this device.
System Description	Shows the type of device. (E.g. Web Smart Managed Switch)
Location	User-defined location for the switch.
Contact	Contain contact details for support.
Device Name	User-defined name for the switch.

System Up Time	Switch's operating time from the time it is switched on. Format is in "day, hour, minute and second".
Current Time	Shows system time of the switch. Format is in "day of the week, month, day of the month, hours: minutes: seconds, year". E.g. "Wed May 17 12:10:11 2007".
BIOS Version	The version of BIOS for the switch.
Firmware Version	The firmware version for the switch.
Hardware-Mechanical version	The version of the hardware and mechanical. The figure prior to the hyphen is the version of electronic hardware and on the other side is the version for mechanical.
Serial Number	The serial number is assigned by the manufacturer.
Host IP Address	The IP address of the switch.
Host MAC Address	Ethernet MAC address of the management agent for the switch.
Device Port	Show all types and numbers of ports.
RAM Size	The size of the DRAM for the switch.
Flash Size	The size of the Flash memory for the switch.

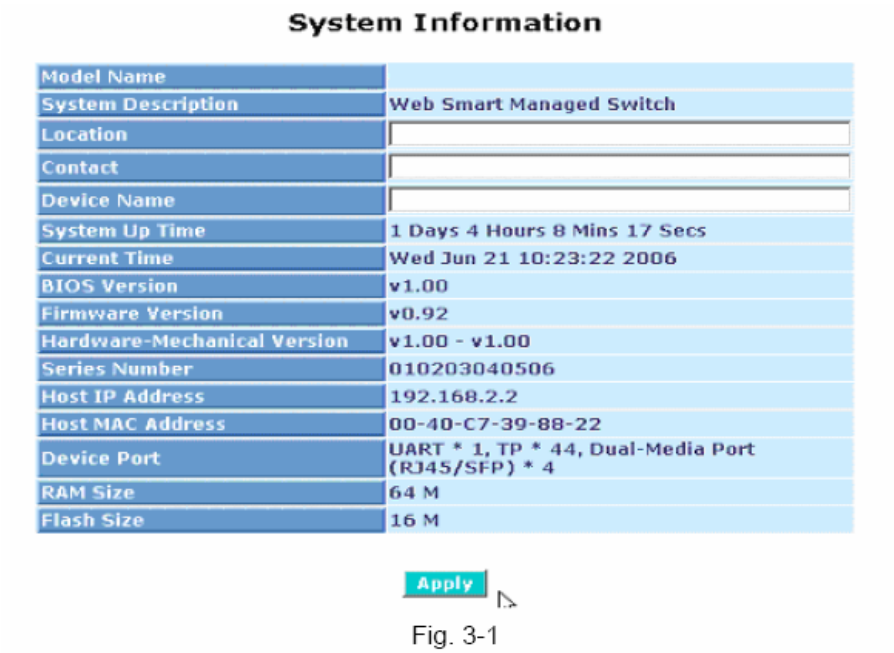


Fig. 3-1

Fig. 3.1 System Information

3.1.2 IP Configuration

Please ensure all PCs connected to the switch are set to the same IP and subnet range. Otherwise, the network manager won't be able to manage or view the device. The IP of the switch can be manually altered and the device will need to be rebooted for the effect to take place.

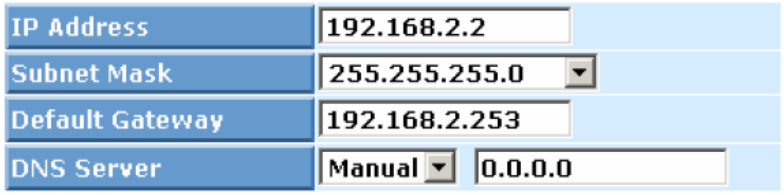


Fig 3.2 IP Configuration

Parameter	Description
IP address	IP settings can be altered when DHCP function is set to "Disable". Then, click **<Apply>** button to update the IP address. If DHCP is enabled, this field will be inaccessible by user. *Default: 192.168.1.1 (DHCP disabled)*
Subnet Mask	Subnet mask is used for increasing IP addresses in a network, since any IP devices in a network need their own IP. Ensure that all devices in the same network have the same subnet values.
Default Gateway	Allocate an IP address for a gateway to manage packets that do not meet routing rules predefined by the switch. *Default: 192.168.1.254*
DNS Server	Domain Name Server acts as a translation between IP address and name address. User can specify a DNS IP address for translating a mnemonic name address into an IP address. • Fixed Mode: user manually specifies IP address. • Dynamic Mode: DHCP server defines the IP address. *Default: 0.0.0.0*

3.1.3 Time Configuration

The system time can be either manually entered or automatically set via NTP. Manual setting allows user to specify the "Year", "Month", "Day", "Hour", "Minute" and "Second". If an invalid input is being assigned, the system will automatically alter the value into a valid range.

NTP is a common protocol used to synchronize the system time between the switch and network. NTP version adopted by the switch is protocol 3 defined in RFC 1305. The switch provides four built-in NTP server IP addresses resided in the Internet and allows extra field for user-defined NTP server IP address. The time zone is in Greenwich-centered format, which uses the expression form of GMT+/- xx hours.

Parameter	Description
Current Time	Display the current time of the system.
Manual	This function allows user to manually specify system time. Filling valid values in each field and click **<Apply>** to update the time. *Default: Year = 2000, Month = 1, Day = 1* *Hour = 0, Minute = 0, Second = 0* *Setting Range:* *Year: >=2000* *Month: 1-12* *Day: 1-31* *Hour: 0-59* *Minute: 0-59* *Second: 0-59*
NTP	Network Time Protocol is used to sync the network time based on Greenwich Mean Time (GMT). Selecting a built-in NTP time server or manually specify a user-defined NTP server with Time Zone, the switch will sync the time after pressing **<Apply>** button. If Time Zone is entered, it will offset GMT and calculate the local time accordingly. The switch supports configurable time zone from -12 to +13 step 1 hour. *Default Time Zone: +8Hrs*
Daylight Saving	Once enabled, it will adjust the time lag or advance in unit of hours according to starting date and ending date. If value is set to one hour, the system time will increase by one hour after one minute past the starting time. When time passes over the ending time, the system time will decease by one hour. Valid value is between

	-5 ~ +5 step one hour. Leaving this value zero will disable the day light saving function. Once day light saving value is set non-zero, it is necessary to set the starting/ending date for the function to activate. *Default:* *Daylight Saving = 0* *Day Light Saving Start* *Mth = 1 (1~12)* *Day = 1 (1~31)* *Hour = 0 (0~23)* *Day Light Saving End* *Mth = 1 (1~12)* *Day = 1 (1~31)* *Hour = 0 (0~23)*

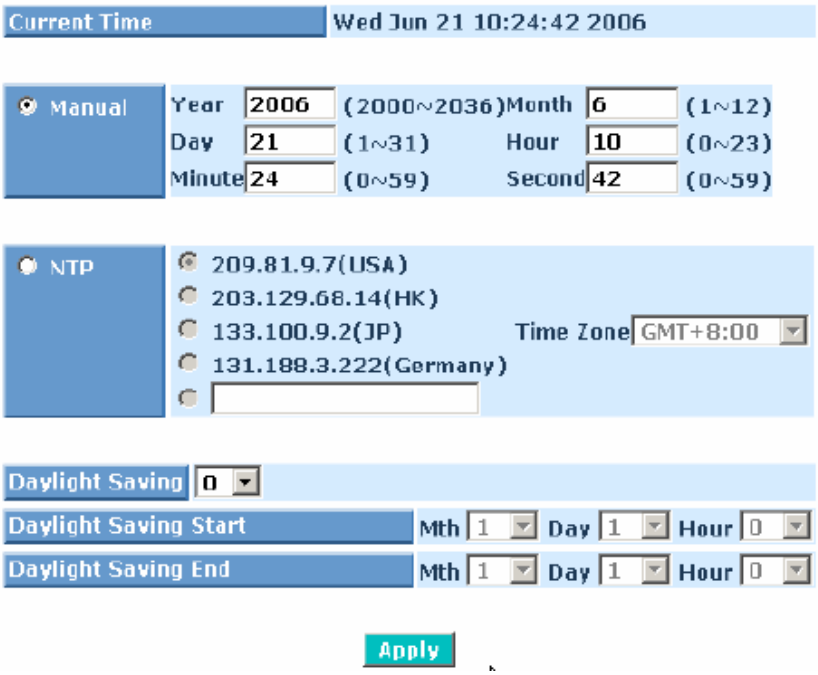


Figure 3.3 Time Configuration

3.1.4 Account Configuration

User accounts are managed in this section where the administrator has the authority to create, modify or delete username and password. Administrator can bypass authentication process when modifying guest identities' password. However, administrator-equivalent identify will require to verifying authority at all times. Only one administrator is allowed and cannot be deleted. In addition, four guest accounts can be created.

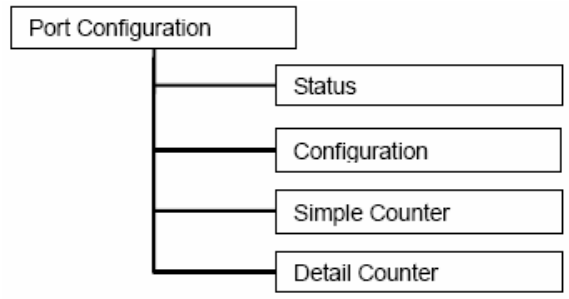
Default for Administrator:
Username: admin
Password: admin

Default for Guest:
Username: guest
Password: guest

Figure 3.4 Account Configuration

3.2 Port Configuration

The following functions will be explained in details in the upcoming sections.



3.2.1 Port Status

This function is the reporting tool that displays status of all ports.

Port No	Media	Link	State	Auto Nego.	Speed/Duplex	Flow Control	
						Transmit	Receive
1	TP	Down	Disabled	Enabled	1G/Half	Enabled	Enabled
2	TP	Down	Enabled	Enabled	1G/Half	Enabled	Enabled
3	TP	Down	Enabled	Enabled	1G/Half	Enabled	Enabled
4	TP	Down	Enabled	Enabled	1G/Half	Enabled	Enabled
5	TP	Down	Enabled	Enabled	1G/Half	Enabled	Enabled

Figure 3.5 Port Status

Parameter	Description
Port No.	Display the port number from 1-48. Port 45-48 are optional modules.
Media	Display the media type adopted by the port. Port 45-48 support either fiber or UTP media for 10/100/1000Mbps.
Link	Indicate whether port is active or not. If port is connected properly to a device, the link will display “UP”, otherwise it will show “Down”.
State	Allow the user to enable or disable the traffic. Once, traffic is set to “Disabled”, data transfer is prevented on this port. *Default: ‘Enable’*
Auto Nego.	Display the exchange mode of Ethernet MAC. If this field is enabled, the switch will automatically negotiate to determine the speed and duplex mode. When the function is disabled, both sides will require the same speed and duplex settings for the link to activate.

Speed/Duplex	Display the speed and duplex of all ports. Switch support data rates of 10/100/1000Mbps and duplex mode of half duplex of full duplex. 1Gbps fiber media only supports 1000Mbps. *1000M TP – NWay: On/Off,* *Speed: 10/100/100M* *Duplex: Full for all, Half for 10/100M* *1000M Fiber – Nway: On/Off* *Speed: 1000M* *Duplex: Full*
Flow Control	This parameter allows flow control on both incoming and outgoing data. If flow control is set as 'Enable' on some port, the port will send PAUSE frame to the transmitting device(s) as the receiving port unable to handle data. For ports that receive pause frames, it will decrease in transmission speed. When it is set as 'Disable', there will be no flow control capability in the port. The packet will be dropped if it is overwhelmed by data. *Default:* *Transmit = 'Enable.'* *Receive = 'Enable'.*

3.2.2 Simple Counter

The function collects information and provides the counting for port traffic, regardless of the packet conditions. The table will contain a summary of all ports' activities. Each data field is 20-digit long and will reset if the amount overflows. The data is updated according to the time interval defined by the user. The valid range for refresh interval is between 3 to 10 seconds and the default is set at 3 seconds.

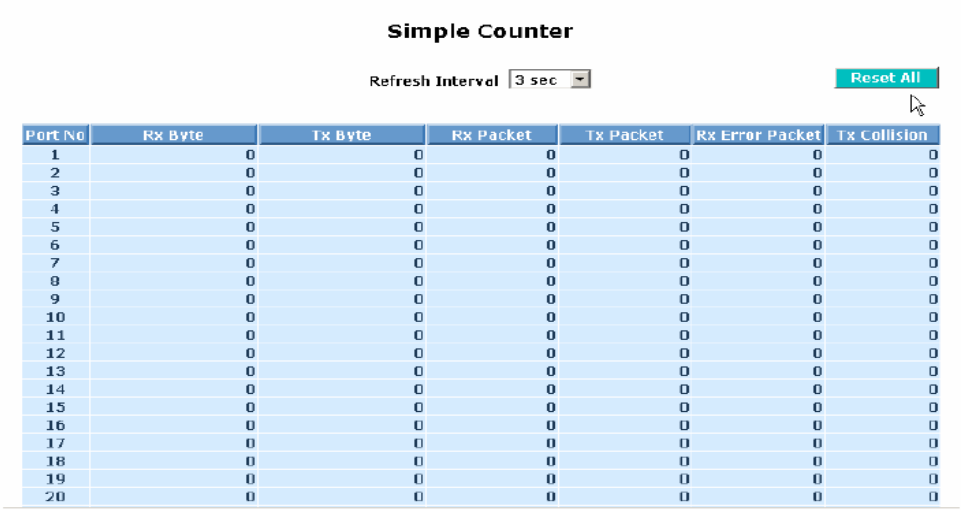


Figure 3.6 Simple Counter

Parameter	Description
Rx Byte	Total received bytes.
Tx Byte	Total transmitted bytes.
Rx Packet	Amount of packets received.
Tx Packet	Amount of packets transmitted.
Rx Error Packet	Amount of bad packets received.
Tx Collision	Amount of collision transmitting frames experienced.

3.2.3 Detail Counter

The function collects any information and provides the counting of port traffic in detail, regardless of packet conditions. The window will only show single port information. To see another port's information, pull down the list from the 'Select' field to change the port to be displayed. Each data field is 20-digit long and will reset if the amount overflows. The data is updated according to the time interval defined by the user. The valid range for refresh interval is between 3 to 10 seconds and the default is set at 3 seconds.

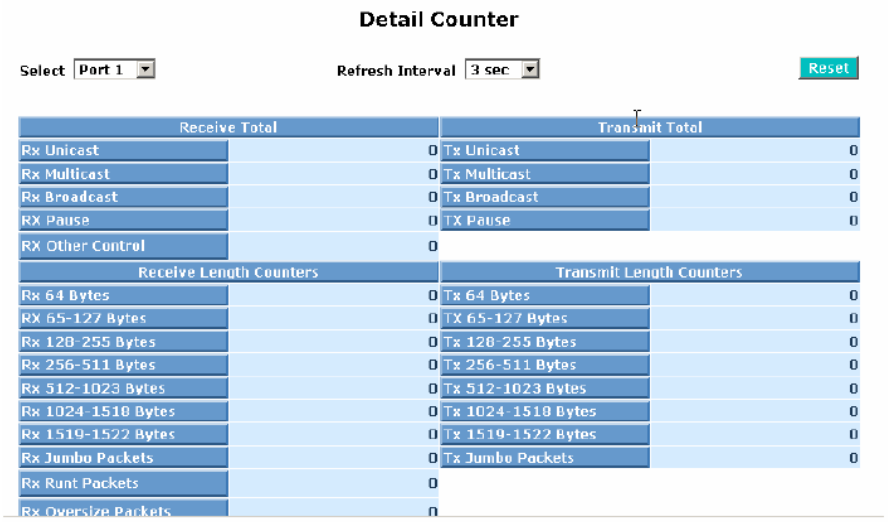


Figure 3.7 Detail Counter

Parameter	Description
Rx Unicast	Amount of unicast packets received.
Rx Broadcast	Amount of broadcast packets received.
Rx Multicast	Amount of multicast packets received.
Rx Pause	Amount of pause frames received.
Rx Other Control	Amount of other type of packets received.
Tx Unicast	Amount of unicast packets transmitted.
Tx Broadcast	Amount of broadcast packets transmitted.
Tx Multicast	Amount of multicast packets transmitted.
Tx Pause	Amount of pause frames transmitted.
Rx 64 Bytes	Amount of 64 bytes for both good and bad packets received.
Rx 65-127 Bytes	Amount of 65~127 bytes for both good and bad packets received.
Rx 128-255 Bytes:	Amount of 128~255 bytes for both good and bad packets received.
Rx 256-511 Bytes	Amount of 256~511 bytes for both good and bad packets received.
Rx 512-1023 Bytes:	Amount of 512~1023 bytes for both good and bad packets received.
Rx 1024-1518 Bytes:	Amount of 1024~1518 bytes for both good and bad packets received.
Rx 1519-1522 Bytes:	Amount of 1519~1522 bytes for both good and bad packets received.
Rx Jumbo Packets:	Amount of packets which are up to 6 times the size of standard Ethernet packets. This field will show amount of Jumbo frames received.
Rx Runt Packets:	Collisions can generate runt packets that are less than 512 bits in length. This field will show the amount of Runt Packets.
Rx Oversize	Amount of long frames (according to max_length) with valid CRC.
Tx 64 Bytes	Amount of 64 bytes for both good and bad packets transmitted.
Tx 65-127 Bytes	Amount of 65~127 bytes for both good and bad packets transmitted.
Tx 128-255 Bytes	Amount of 128~255 bytes for both good and bad packets transmitted.
Tx 256-511 Bytes	Amount of 256~511 bytes for both good and bad packets transmitted.
Tx 512-1023 Bytes	Amount of 512~1023 bytes for both good and bad packets transmitted.
Tx 1024-1518 Bytes	Amount of 1024~1518 bytes for both good and bad packets transmitted.
Tx 1519-1522 Bytes	Amount of 1519~1522 bytes for both good and bad packets transmitted.
Tx Jumbo Packets	Amount of packets which are up to 6 times the size of standard Ethernet packets. This field will show amount of Jumbo frames transmitted.

Rx CRC	Amount of Alignment errors and CRC error packets received.
Rx Code	Amount of packets received with a CRC error and a code error. These packets do not have dribble bits and are at least 64 bytes in length.
Rx Fragment	Amount of short frames (< 64 bytes) with invalid CRC.
Tx Single Collisions	Amount of packets successfully transmitted after experiencing one collision.
Tx Multiple Collisions	Amount of packets successfully transmitted after experiencing multiple collisions.
Tx Excessive Collisions	Amount of packets successfully transmitted after experiencing excessive collisions.
Tx Late Collisions	Amount of packets that fail to be transmitted due to a late collision. Such packets may have experienced one or more normal collisions prior to the late collision.
Tx Deferred	Amount of all packets that had to defer to either traffic on the network (half-duplex mode) or to an active pause timer (full-duplex mode).

3.3 Storm

3.3.1 Storm Control

Storm Control is used to block unnecessary frames of the multicast and broadcast reducing the switch's performance. When the frames of the multicast or broadcast are over the rate and with Strom Control enabled, it will drop the frames of exceeded rate.

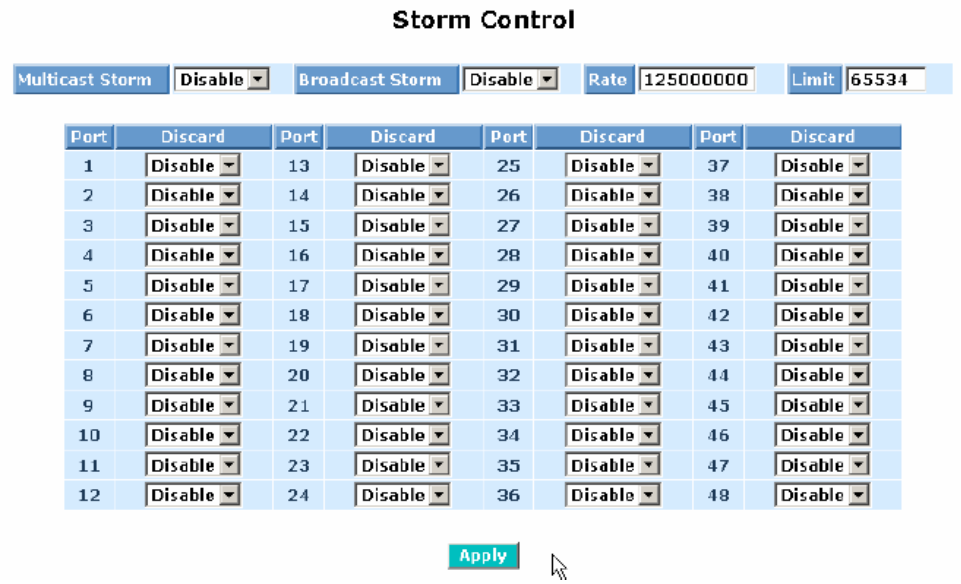


Figure 3.8 Storm Control

Parameter	Description
Multicast Storm	To enable the Multicast Storm capability. *Default: 'Disable'.*
Broadcast Storm	To enable the Broadcast Storm capability. *Default: 'Disable'.*
Rate	The transmitting rate of Multicast or Broadcast packets. *Default: 125000000 bytes.* *Setting range: 119~125000000.*
Limit	Limit size for buffer of the switch and the maximum tolerated packets. *Default: "65534"*
Port	Select port 1~48 for applying Strom Control.

Discard	To discard the frames of the multicast or broadcast exceeding the rate of Storm Control's configuration. After completing the function's setting, click **<Apply>** button to have this function to take effect. *Default: 'Disable'.*

3.4 Mirror

3.4.1 Mirror Setting

Mirror Configuration is to monitor the traffic of the network. For example, assume that Port A and Port B are ‘Monitoring Port’ and ‘Monitored Port’ respectively, the traffic received by Port B will be copied to Port A for monitoring.

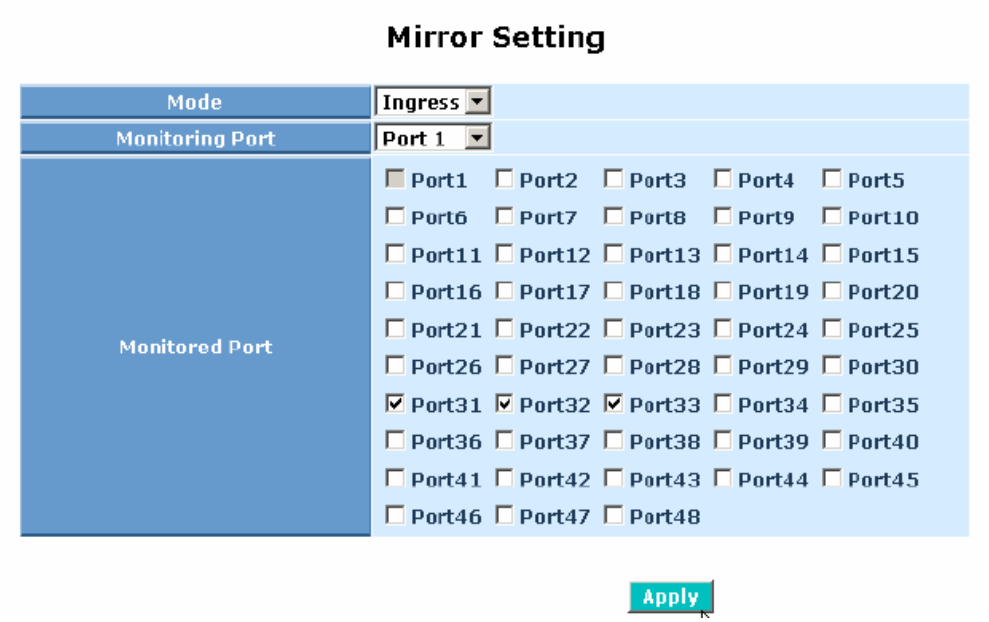


Figure 3.9 Mirror Setting

Parameter	Description
Mode	Decide the modes of mirror: ‘Disable’, ‘Ingress’ and ‘Egress’.
Monitoring Port	To select the monitoring port. Valid port is 1~48. *Default: None.* *Setting Range: 1~48.*
Monitored Ports	To select the ports to be monitored. Valid port is 1~48. Tick the check box ( ) beside the port and click **<Apply>** button.

3.5 Filter

3.5.1 Filter Setting

Filter Setting can prevent the switch from abnormal or unknown traffic and increase switch's performance. It can filter the network traffic from 'Bad Length' packet, 'Unknown Encapsulation' packet, 'Unknown EtherType' frame, 'Unknown IP Protocol' packet, IPv4 options packet and 'Unknown Source Address' packet.

Parameter	Description
Filter Mode	Bad Length is a packet received with length field that does not match the length of the packet's data field. Unknown Encapsulation is a packet received with encapsulation that is not Ethernet V2 or SNAP (with or without VLAN tag). Unknown EtherType is a packet received with field that is not IPv4, IPv6, ARP, or RARP. Unknown IP Protocol is a packet received with IP protocol field that is not ICMP, IGMP, TCP or UDP.
Ports	Port 1-48 are available for filtering. Ticking options (L.) are used to filter the traffic of the logical ports created by Link Aggregation. Tick "All" will click all physical ports rapidly. After completing the function's setting, click **<Apply>** button.

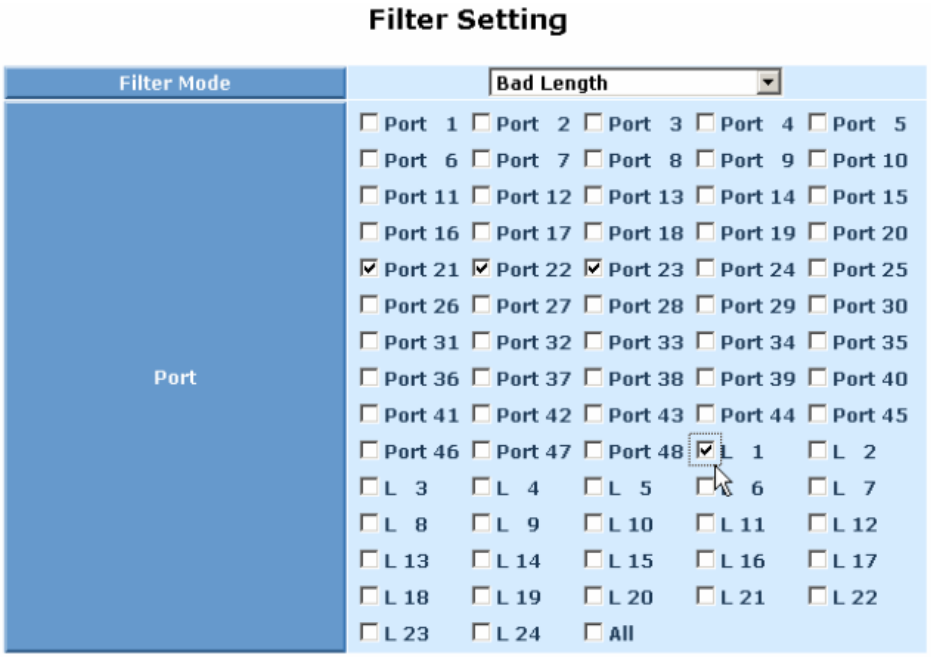
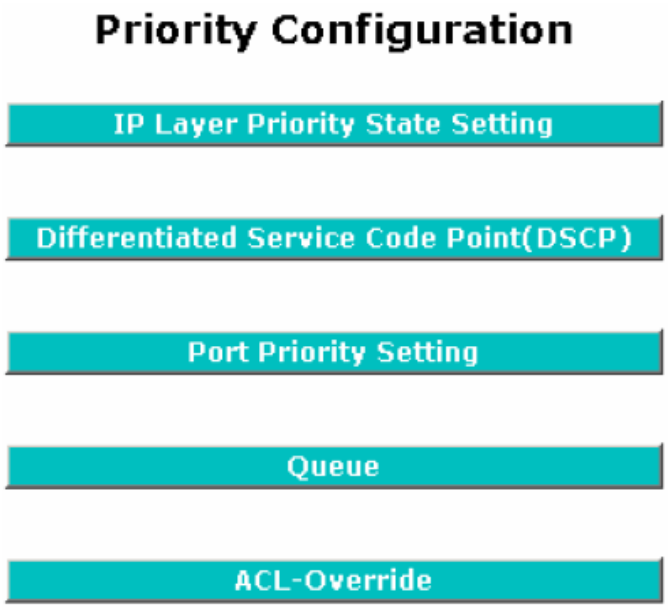

Filter Setting
Filter Mode
Bad Length
Port
Port 1 Port 2 Port 3 Port 4 Port 5
Port 6 Port 7 Port 8 Port 9 Port 10
Port 11 Port 12 Port 13 Port 14 Port 15
Port 16 Port 17 Port 18 Port 19 Port 20
Port 21 Port 22 Port 23 Port 24 Port 25
Port 26 Port 27 Port 28 Port 29 Port 30
Port 31 Port 32 Port 33 Port 34 Port 35
Port 36 Port 37 Port 38 Port 39 Port 40
Port 41 Port 42 Port 43 Port 44 Port 45
Port 46 Port 47 Port 48 L 1 L 2
L 3 L 4 L 5 L 6 L 7
L 8 L 9 L 10 L 11 L 12
L 13 L 14 L 15 L 16 L 17
L 18 L 19 L 20 L 21 L 22
L 23 L 24 All

Figure 3.10 Filter Setting

3.6 QOS

3.6.1 Priority Configuration

There are five settings available for Priority Configuration. In the switch, there are three modes of QoS: DSCP, 802.1p and Port Priority respectively. The precedence of them are DSCP > 802.1p > Port Priority. For 802.1p or Port Priority mode, these ports should enable IP-ignored in advance. Furthermore, the scheduling of QoS uses Strict Priority and the higher priority of packet will get the highest precedence to transit in the switch. In Priority Configuration, for ACL to override other priorities of QoS, enable 'ACL-enabled' in some ports. 802.1p is the priority of VLAN tag.



3.6.2 IP Layer Priority State Setting

The setting allows DSCP (IP Layer) to be disabled and the 802.1p or Port Priority to take effect. DSCP has higher precedence than 802.1p and Port Priority and it is necessary to enable IP-ignore function.

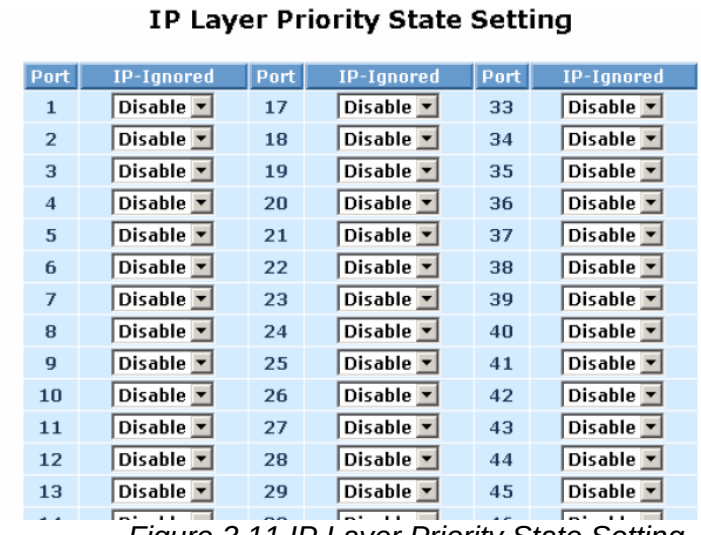

IP Layer Priority State Setting
Port IP-Ignored Port IP-Ignored Port IP-Ignored
1 Disable 17 Disable 33 Disable
2 Disable 18 Disable 34 Disable
3 Disable 19 Disable 35 Disable
4 Disable 20 Disable 36 Disable
5 Disable 21 Disable 37 Disable
6 Disable 22 Disable 38 Disable
7 Disable 23 Disable 39 Disable
8 Disable 24 Disable 40 Disable
9 Disable 25 Disable 41 Disable
10 Disable 26 Disable 42 Disable
11 Disable 27 Disable 43 Disable
12 Disable 28 Disable 44 Disable
13 Disable 29 Disable 45 Disable

Figure 3.11 IP Layer Priority State Setting

Parameter	Description
IP-ignored	Enable this function for ports will disable DSCP for QoS.

3.6.3 Differentiated Service Code Point (DSCP)

Differentiated Service Code Point (DSCP) function could form total of 64 (0~63) kinds of Traffic Class based on the arrangement of 6-bit field in DSCP of the IP packets. In the switch, users are allowed to set up 64 kinds of Class that belong to any of 0~7 Priority. The switch supports 8 kinds of priorities and 4 Queues.

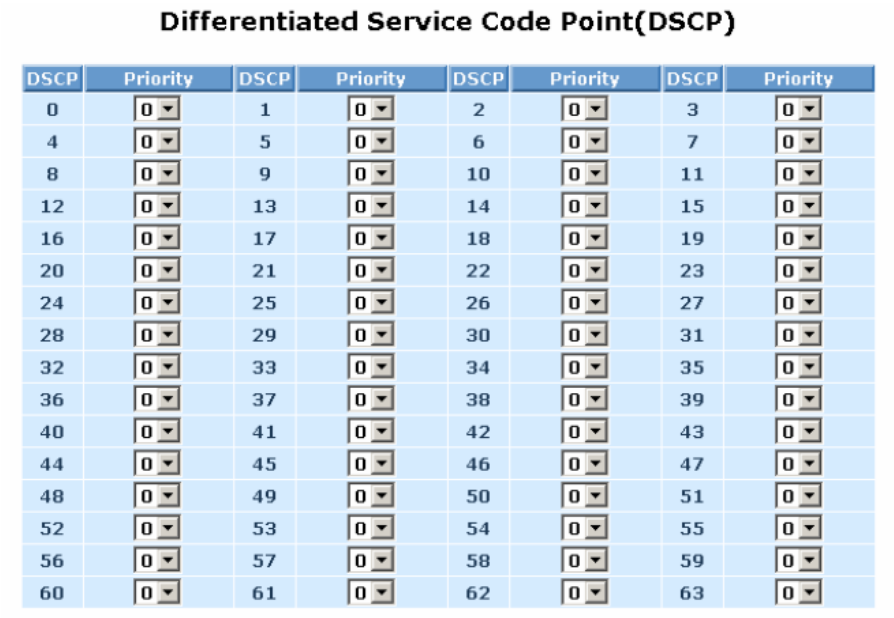
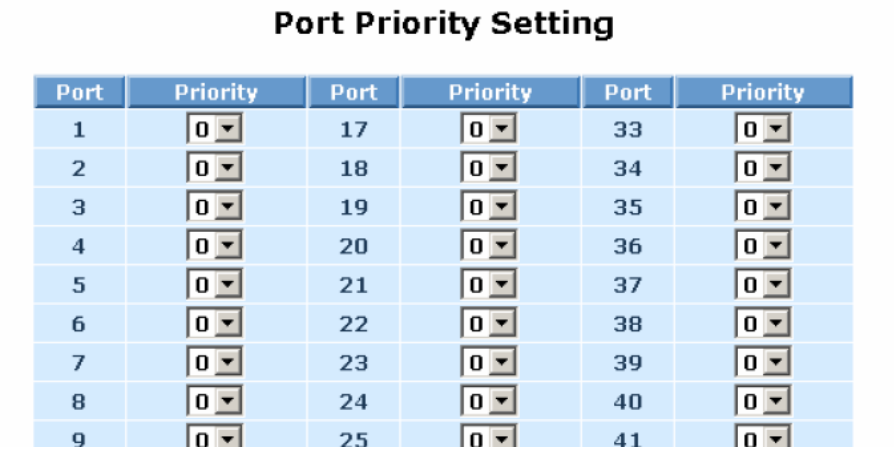


Figure 3.12 DSCP

Parameter	Description
DSCP	0~63 DSCP priorities available.
Priority	0~7 Priority for each DSCP.

3.6.4 Port Priority Setting

Allow users to set the priority of each port.



Parameter	Description
Priority	0~7 Priority for each port.

3.6.5 Shaper Queue

The switch supports 4 queues (0-3) for Shaper function controlling. Any of 0~7 Priority could be mapped to any of 0~3 queue. After determining the queue of each priority, the function will influence QoS scheduling and Shaper Queue when packets are transmitted. The QoS scheduling is Strict Priority. When all priorities are entered into the same queue, there will be no effect on Strict Priority.

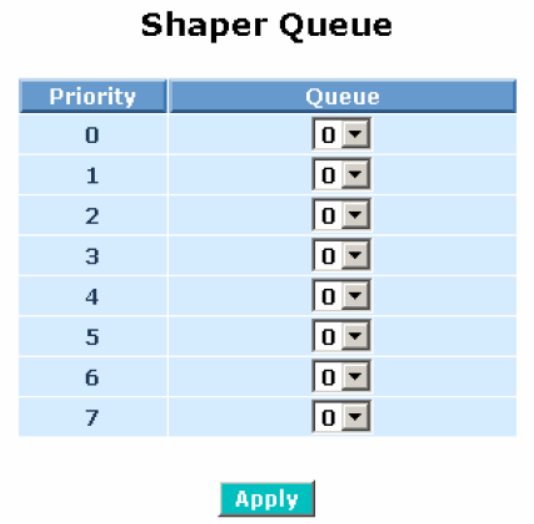


Figure 3.13 Shaper Queue

Parameter	Description
Priority	The switch supports 0~7 Priority.
Queue	Any 0~7 Priority can be assigned to 0~4 Queue.

3.6.6 ACL Priority Override

The switch allows users to set ACL priority have the higher precedence for each port in ACL Priority Override function. If ACL-Override is enabled, the other QoS priority of DSCP, 802.1P, and Priority will be revealed.

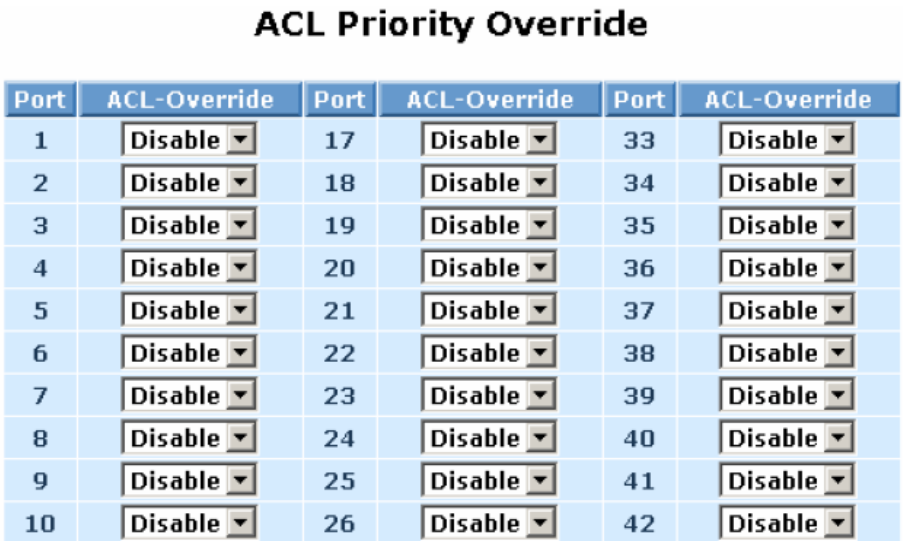

ACL Priority Override
Port ACL-Override Port ACL-Override Port ACL-Override
1 Disable 17 Disable 33 Disable
2 Disable 18 Disable 34 Disable
3 Disable 19 Disable 35 Disable
4 Disable 20 Disable 36 Disable
5 Disable 21 Disable 37 Disable
6 Disable 22 Disable 38 Disable
7 Disable 23 Disable 39 Disable
8 Disable 24 Disable 40 Disable
9 Disable 25 Disable 41 Disable
10 Disable 26 Disable 42 Disable

Figure 3.13 ACL Priority Override

Parameter	Description
ACL-override	Any port set to 'Enable', ACL Priority will take effect over other QoS priority.

3.6.7 Policer Configuration

When the packets are injected into the switch (Ingress Ports) and match Flow ID entry, Flow ID will decide which priority to take effect according to Policer Flow ID table. Packets will be allowed or discarded according to the transmitting rate corresponding to the rate setting in Policer Configuration.

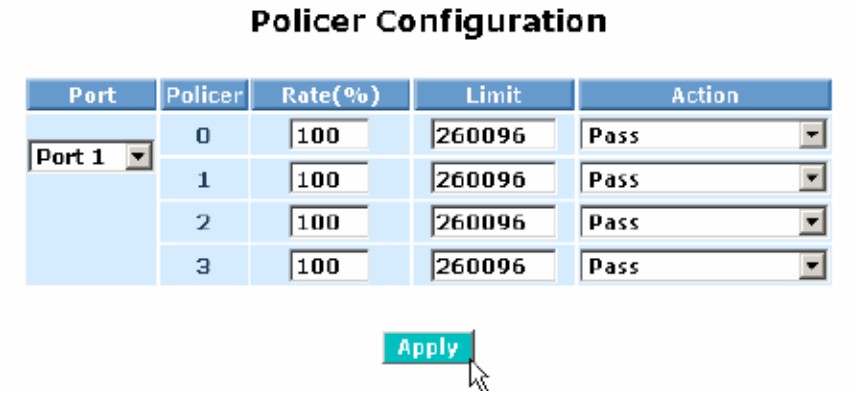


Figure 3.14 Policer Configuration

Parameter	Description
Port	Port 1~48 are available for Policer Configuration.
Policer	0~3 Policer are available to accompany the 4 queues of ingress ports.
Rate	The rate bound is the limit for 0~3 Policer and setting range is 0~100%.

Limit	The burst number of packets for admission to the switch for each Policer and it is in buffer size of Ingress ports. *Default: 260096 bytes.* *Setting Range: 2048~260096 bytes.*
Action	There are four actions for Policer Configuration: Pass, Discard-congested, Discard and Demote. “Pass” setting will let packets enter the switch successfully on ingress ports regardless of the rate. “Discard” setting is when packets reach the rate setting in Policer Configuration function, it will be discarded immediately. “Discard-congested” setting refers to the packets that cause congestion when entering the switch will be discarded. “Demote” setting refers to amount of packets entering the switch reaches the rate, the priority of the packets will be decided and changed again in Mark function. According to demote setting and the priority of the packets when these ports enable Mark will affect 802.1p (CoS) and DSCP.

3.6.8 Shaper Setting

When packets are passed through the switch (Egress Ports), packets will be entered into Egress queue and be influenced by limiting rate of the Shaper Configuration. Shaper Queue function will determine which egress queue the packet belong.

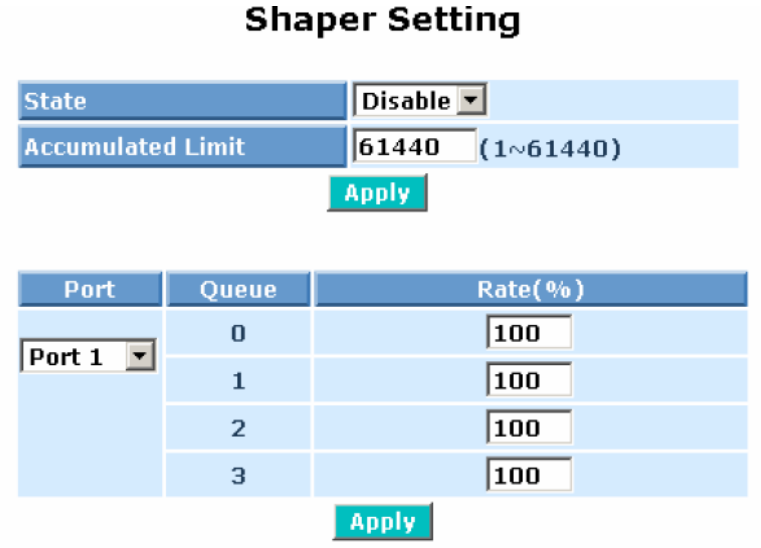
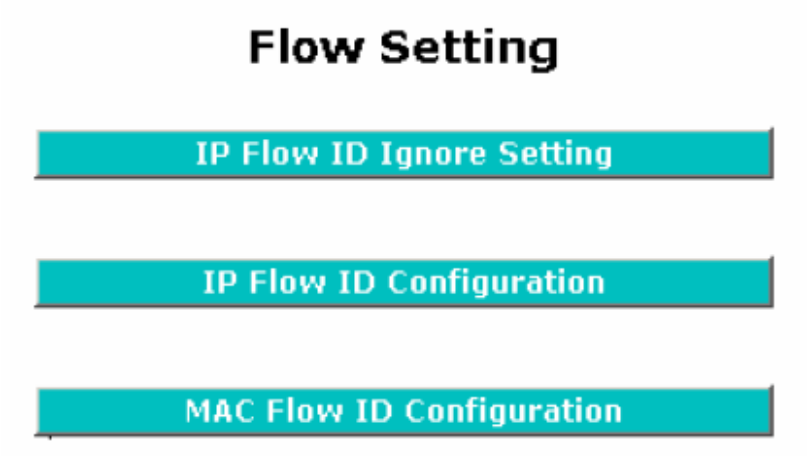


Figure 3.15 Shaper Setting

Parameter	Description
State	The selection for enabling Shaper function. *Default: 'Disable".*
Accumulated	The maximum packets transmitted out of the switch. *Default: 61440* *Setting Range: 1-61440*
Port	Select the port to apply Shaper function. *Setting Range: 1~48*
Queue	Each port has 4 Queue for applying Shaper function.
Rate	Transmitting rate out of switch. *Setting Range: 0~100%.*

3.6.9 Flow

When the packet enters the switch, it will be mapped to a proper flow ID according to the IP Flow ID Configuration or MAC Flow ID Configuration. The priorities of packets will agree with the setting in Policer Flow ID Table and are controlled by suitable policer (Policer 0~3).



3.6.10 IP Flow ID Ignore Setting

This section will allow users to cancel the effects of IP Flow ID and to use the MAC Flow ID. Enable the “IP Flow ID Ignore” to use MAC Flow ID.

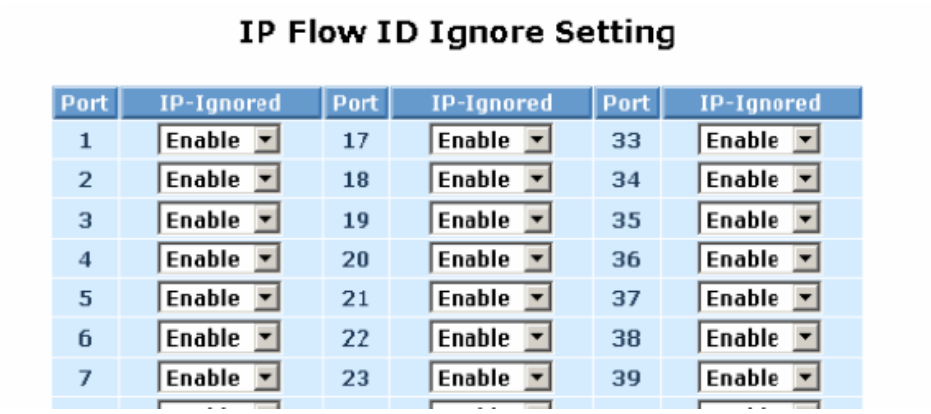


Figure 3.16 IP Flow ID Ignore Setting

Parameter	Description
IP-ignored	Allow the setting for ‘IP Flow ID ignore’. Click **<Apply>** for the changes to take effect. *Default: ‘Disable’.*

3.6.11 IP Flow ID Configuration

In IP Flow ID Configuration, click **<Add>** button to create IP Flow ID Configuration entry. When the IP packet enters the switch and fit the IP Flow ID Configuration, user can check Policer Flow ID Table to find which priority should be mapped to the proper policer. After IP Flow ID setting, press **<Apply>** button in “ACL QoS Load” function to take effect.

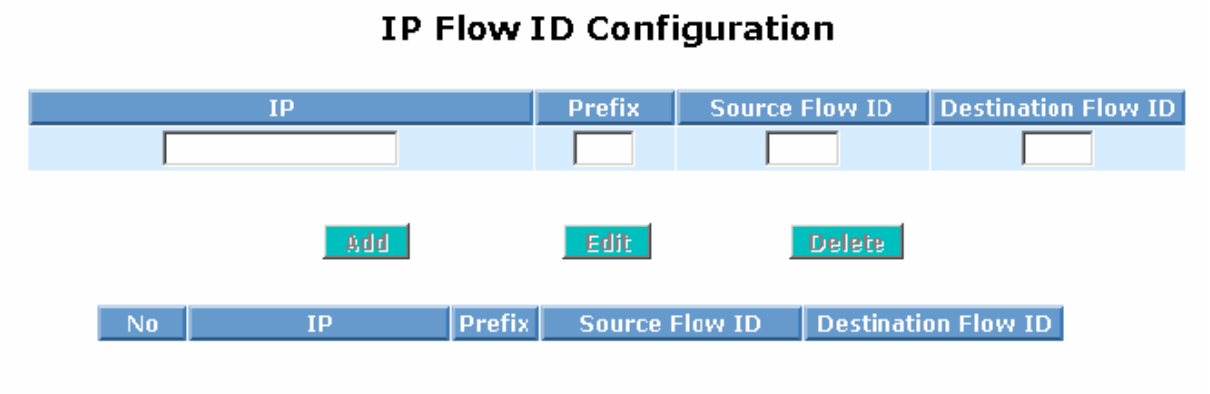


Figure 3.17 IP Flow ID Configurations

Parameter	Description
IP	*Setting Range: 0.0.0.0 ~ 255.255.255.255*
Prefix	If the IP packets are inside IP range and co-operating with Prefix, packets will be influenced by this IP Flow ID Configuration. *Setting Range: 1~32.*
Source Flow ID	*Setting Range: 0~3.*
Destination Flow ID	*Setting Range: 0~3.*

3.6.12 Static Forwarding MAC

Click **<Add>** button to create MAC Flow ID Configuration entry. When packets enter the switch and fit the MAC Flow ID Configuration, users can check Policer Flow ID Table to find which priority should be mapped to the proper policer. After Static Forwarding MAC setting, press **<Apply>** button in “ACL QoS Load” function to take effect.

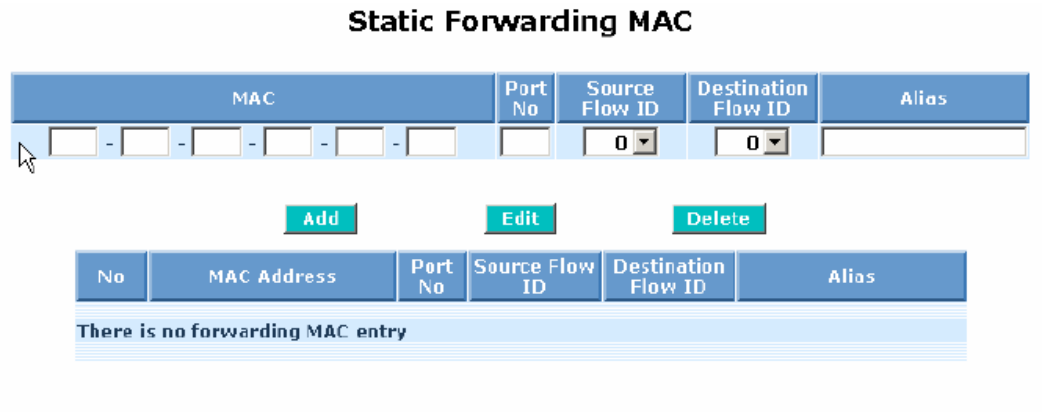


Figure 3.18 Static Forwarding MAC

Parameter	Description
MAC	MAC setting must be unicast. *Setting Range: 00-00-00-00-00-00 ~ ff-ff-ff-ff-ff-fe*
Port No	*Setting Range: 1~48.*
Source Flow ID	*Setting Range: 0~3.*
Destination Flow ID	*Setting Range: 0~3.*
Alias	Any Unicode can be entered.

3.6.13 Policer Flow ID Table

This section is for IP Flow ID Configuration and MAC Flow ID Configuration to map and decide appropriate Policer.

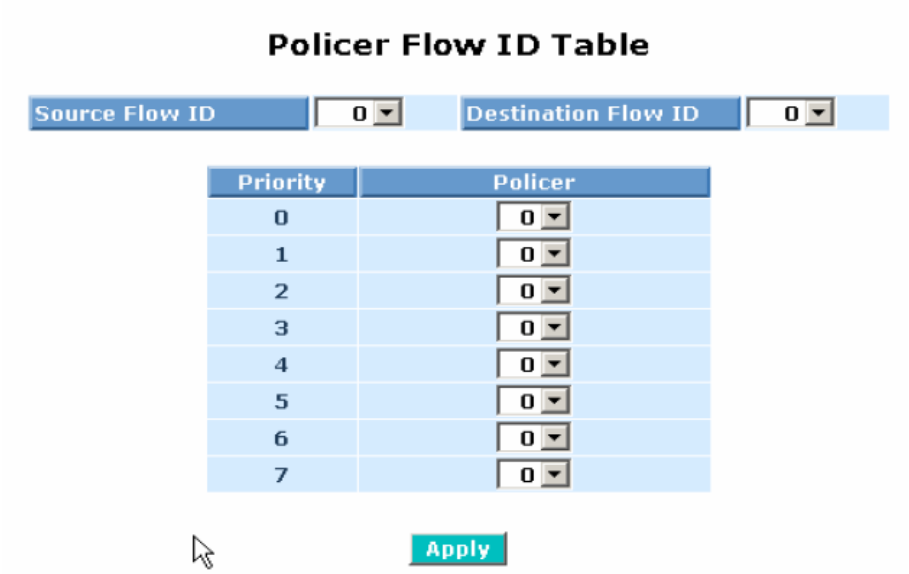


Figure 3.19 Policer Flow ID Table

Parameter	Description
Source Flow ID	Click **<Apply>** to have the setting take effect. *Setting Range: 0~3.*
Destination Flow ID	Click **<Apply>** to have the setting take effect. *Setting Range: 0~3.*
Priority	*Setting Range: 0~7.*
Policer	There are 0~3 Policer for each Priorities. Click **<Apply>** to have the setting take effect.

3.6.14 Mark Priority

In Policer function, users can see the Demote capability in Action list. When the amount of packets reaches the rate and the action is determined as Demote (the queue of ingress port influenced by Policer function), the priority will be decided and changed with the setting of Demoted in Mark Priority function. Furthermore, if the amount of packets doesn't reach the rate of Policer function, these packets will be put in the queues decided by Not-demoted in Mark Priority function. CoS will act on packets of 802.1p QoS, being the priority of VLAN's tag. DSCP is another QoS capability, which affects the priority of IP Packets.

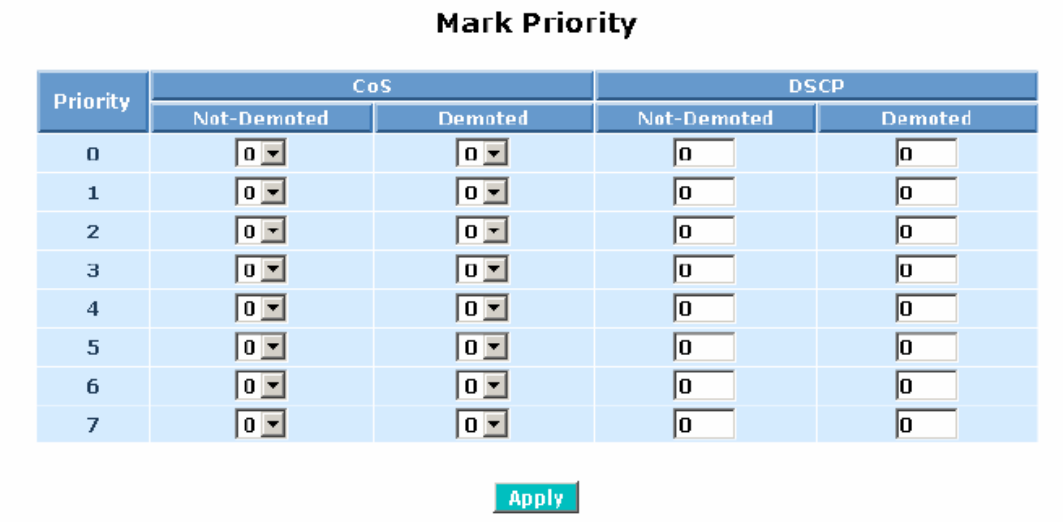


Figure 3.20 Mark Priority

Parameter	Description
Priority	There are 0~7 priorities in the switch.
Not-demoted	There are 0~3 queues for selection in ingress ports not reaching the rate set in Policer function. Click **<Apply>** to have the setting take effect.
Demoted	There are 0~3 queues for selection in ingress ports reaching the rate set in Policer function. Click **<Apply>** to have the setting take effect.

3.6.15 Mark-enable CoS/DSCP

The function allows enabling of Mark function for CoS/DSCP per port.

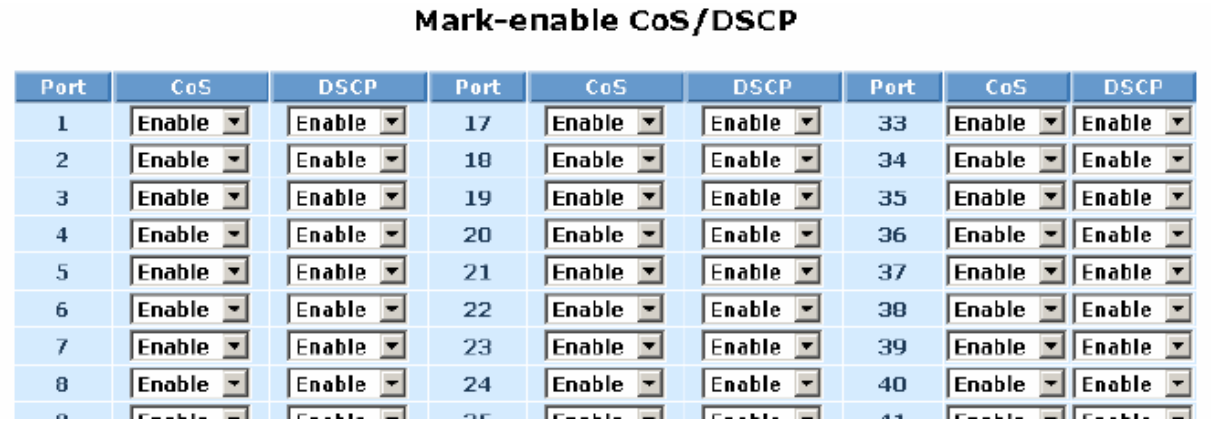

Mark-enable CoS/DSCP
Port CoS DSCP Port CoS DSCP Port CoS DSCP
1 Enable Enable 17 Enable Enable 33 Enable Enable
2 Enable Enable 18 Enable Enable 34 Enable Enable
3 Enable Enable 19 Enable Enable 35 Enable Enable
4 Enable Enable 20 Enable Enable 36 Enable Enable
5 Enable Enable 21 Enable Enable 37 Enable Enable
6 Enable Enable 22 Enable Enable 38 Enable Enable
7 Enable Enable 23 Enable Enable 39 Enable Enable
8 Enable Enable 24 Enable Enable 40 Enable Enable

Figure 3.21 Mark-enable CoS/DHCP

Parameter	Description
CoS	Allow the users to make CoS for QoS effective. Click **<Apply>** to have the setting take effect. *Default: 'Enable'.*
DSCP	Allow the users to make DSCP for QoS effective. Click **<Apply>** to have the setting take effect. *Default: 'Enable'.*

3.6.16 ACL

Access Control List (ACL) is designed to protect the switch from unnecessary IP traffic or Layer-4 packets and allow users to filter denial of service (DoS) floods against the switch. Users can create 64 sets of ACL with two types of mode: Port Mode and VLAN mode. In Port Mode, all 48 ports are mapped to the same ACL number. For example, port 1 will correspond to ACL number 1. However, in VLAN mode, it could choose its own ACL number. Click **<Apply>** button in ACL QoS Load for the function to take effect.

Figure 3.22 ACL Mode

Parameter	Description
ACL Mode	Two types of mode: Port Mode and VLAN mode. Click **<Apply>** to have the setting take effect.

3.6.17 ACL/VLAN Mapping

In this function, users can map the VLAN to the ACL number.

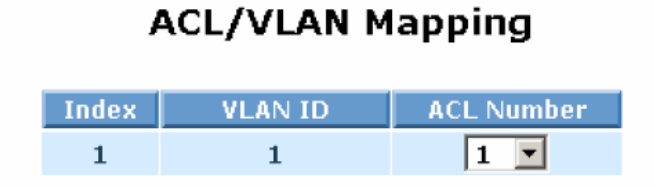


Figure 3.22 ACL Mode

Parameter	Description
VLAN ID	This page will display existing 'VLAN VID'. *Default: VLAN VID = 1.*
ACL Number	Each VLAN ID can be assigned 1~64 ACL Number. Click **<Apply>** to have the setting take effect.

3.6.18 ACL Rule

In this function, users can create the ACL rules in each ACL Number. The smaller index of ACL Rule will have higher effect than the higher index of ACL Rule. Click **<Apply>** in the ACL QoS Load to have the setting take effect.

- Press **<Create>** button to create ACL Rule.
- Press **<Edit>** button to edit ACL Rule.
- Press **<Delete>** button to delete ACL Rule.

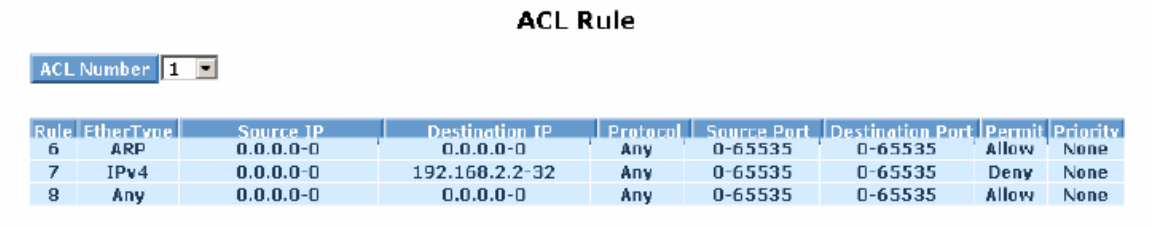

ACL Rule
ACL Number 1
Rule EtherType Source IP Destination IP Protocol Source Port Destination Port Permit Priority
6 ARP 0.0.0.0-0 0.0.0.0-0 Any 0-65535 0-65535 Allow None
7 IPv4 0.0.0.0-0 192.168.2.2-32 Any 0-65535 0-65535 Deny None
8 Any 0.0.0.0-0 0.0.0.0-0 Any 0-65535 0-65535 Allow None

Figure 3.23 ACL Rule

Parameter	Description
Rule	ACL rule index.
EtherType	EtherType is used to indicate the protocol type in Ethernet packets and is coded as 2 bytes.
Source IP	The source of IP address. *Setting Range: 0.0.0.0~255.255.255.255.*
Destination IP	The destination of IP address. *Setting Range: 0.0.0.0~255.255.255.255.*

Protocol	Protocol type in packets.
Source Port	OSI Layer-4 Port number of source location *Setting Range: 0~65535.*
Destination Port	OSI Layer-4 Port number of destination location. *Setting Range: 0~65535.*
Permit	Indicate whether the packets are allowed access or blocked. There are two statuses: Allow or Deny.
Priority	The transmitting precedence. For packets conforming to ACL rule with ACL QoS Load and ACL-override enabled, it will apply this ACL priority. The switch supports 0~7 priority.

3.6.19 ACL Rule Setting

After pressing **<Create>** button in ACL Rule function, ACL Rule setting page will appear on the interface. In this page, users can select suitable settings and press **<Apply>** button to create ACL rule. Click **<Apply>** in the ACL QoS Load to have the setting take effect.

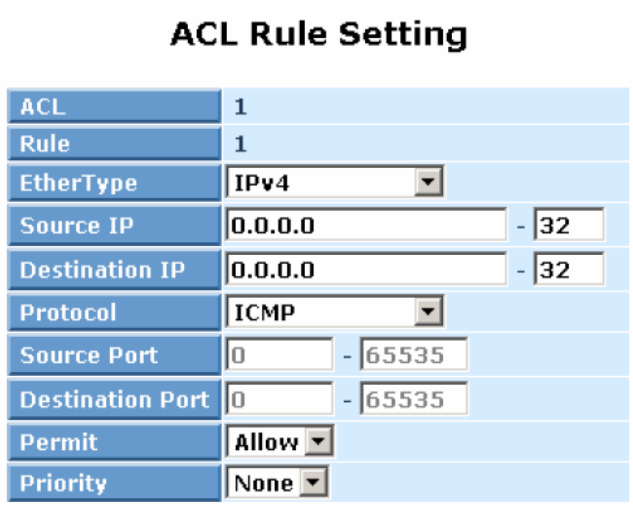


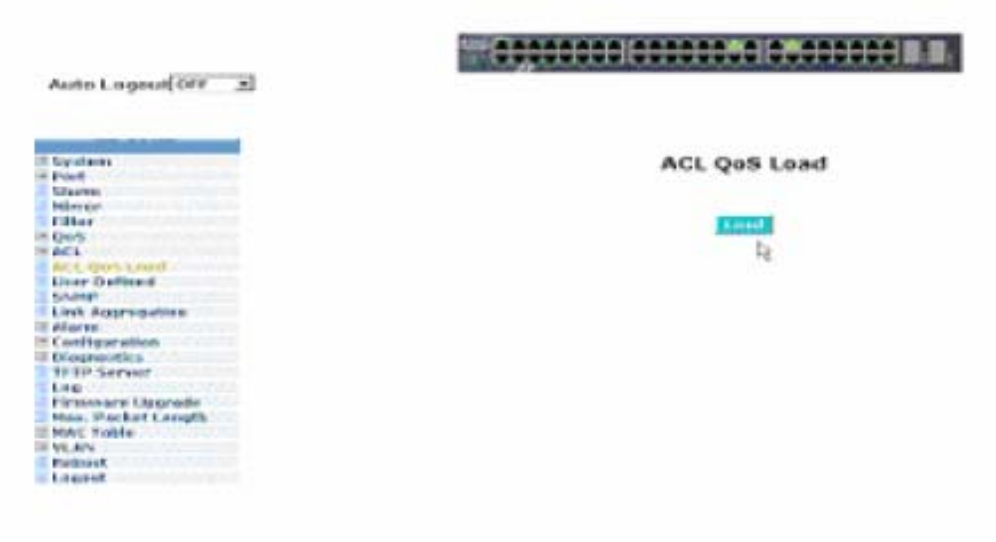
Figure 3.24 ACL Rule Setting

Parameter	Description
ACL	ACL rule number. There are 1~64 ACL numbers.
Rule	ACL rule index.
EtherType	EtherType is used to indicate the protocol type in Ethernet packets and is coded as 2 bytes. Users can select EtherType as IPv4, ARP, RARP, Type 1, Type 2, Type 3, None, or Any. Type 1, 2, 3 are determined by users in User Defined function.

Source IP	The Source of IP address and IP Prefix *IP Range: 0.0.0.0~255.255.255.255.* *IP Prefix Range: 0~32.*
Destination IP	The Destination of IP address and IP Prefix. *IP Range: 0.0.0.0~255.255.255.255.* *IP Prefix Range: 0~32.*
Protocol	Protocol type in packets. Users can select protocol type as ICMP, IGMP, TCP, UDP, Protocol1, Protocol2, Protocol3, None, or Any. Protocol1, Protocol2 and Protocol are determined by users in User Defined function.
Source Port	OSI Layer-4 Port number of source location would be available for setting when Protocol type is either TCP or UDP. *Setting Range: 0~65535.*
Destination Port	OSI Layer-4 Port number of destination location. *Setting Range: 0~65535.*
Permit	Indicate whether the packets are allowed access or blocked. There are two statuses: Allow or Deny.
Priority	The transmitting precedence. For packets conforming to ACL rule with ACL QoS Load and ACL-override enabled, it will apply this ACL priority. The switch supports 0~7 priority.

3.6.20 ACL QoS Load

Enable QoS Capability in ACL function. Click **<Apply>** to have the setting take effect.



3.6.21 User Defined

Users define own values of the EtherType and Protocol. It will become available when creating ACL rule.

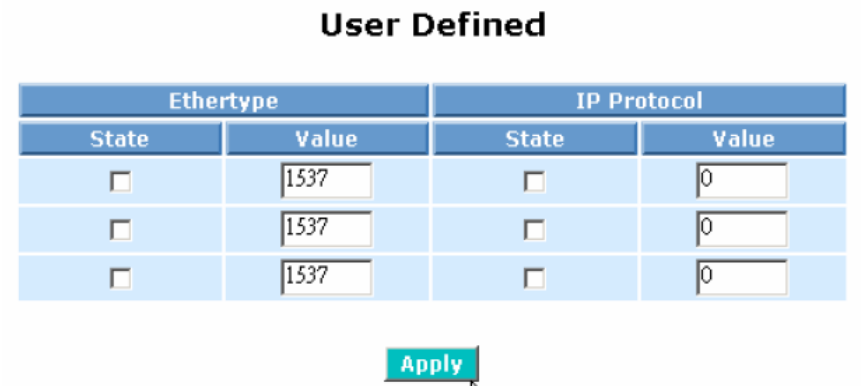


Figure 3.25 User Defined

Parameter	Description
State	Tick the option button to open and fill in the value of EtherType and IP Protocol. Click **<Apply>** to have the setting take effect.
Value	The Value of EtherType and IP Protocol. *Default: EtherType = 1537.* *IP Protocol = 0.*

3.7 SNMP

Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can control the managed devices equipped with SNMP agent, provided that the Management Information Base (MIB) is installed correctly on the managed devices. The SNMP is a protocol that is used to govern the transfer of information between SNMP manager and agent. Also, traverses the Object Identity (OID) of the management Information Base (MIB), described in the form of SMI syntax. SNMP agent is running on the switch to response to the request issued by SNMP manager.

The switch supports an option to turn on or off the SNMP agent. If users set the field SNMP 'Enable', SNMP agent will become active. All supported MIB OIDs, including RMON MIB, can be accessed via SNMP manager. If the field SNMP is set to "Disable", SNMP agent will be de-activated and the related Community Name, Trap Host IP Address, Trap and all MIB counters will be ignored.

3.7.1 SNMP Configuration

This function is used to configure SNMP settings, community name, trap host and public traps. A SNMP manager must pass the authentication by identifying both community names before accessing the MIB information of the target device. Both parties must have the same community name. Click **<Apply>** to have the setting take effect.

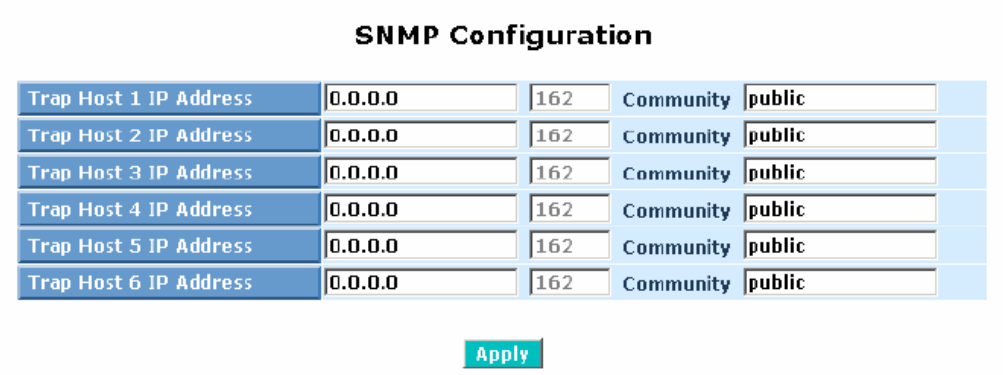

SNMP Configuration
Trap Host 1 IP Address 0.0.0.0 162 Community public
Trap Host 2 IP Address 0.0.0.0 162 Community public
Trap Host 3 IP Address 0.0.0.0 162 Community public
Trap Host 4 IP Address 0.0.0.0 162 Community public
Trap Host 5 IP Address 0.0.0.0 162 Community public
Trap Host 6 IP Address 0.0.0.0 162 Community public
Apply

Figure 3.26 SNMP Configuration

Parameter	Description
SNMP	The parameter is used for the activation or de-activation of SNMP. *Default: 'Enable'.*

Get/Set/Trap Community	Community name is used as password for authentication where the requesting network management unit must belong to a community group. The requesting network management unit cannot access the device with different community name via SNMP protocol. Community name is user-definable with a maximum length of 15 characters and is case sensitive. Community name string must not be left blank. Any printable characters are allowed. The community name for each function works independently. Each function has its own community name. The community name for GET only works for GET function and can't be applied to other function such as SET or Trap. *Default:* *SNMP function = 'Enable'.* *Community name for GET: 'public'* *Community name for SET: 'private'* *Community name for Trap: 'public'* *Set function : 'Enable'* *Trap host IP address: 0.0.0.0* *Port number :162*

3.8 Link Aggregation

The Aggregation Configuration (Port Trunk) is used to configure the settings of Link Aggregation. Users can bundle more than one port with the same speed in full duplex and the same MAC to a single logical port that aggregates the bandwidth of these ports. This means user can apply current Ethernet equipments to build the bandwidth aggregation. For example, if there are three Fast Ethernet ports aggregated in a logical port, then this logical port has bandwidth with three times as high as a single Fast Ethernet port.

3.8.1 Aggregation Configuration

Display the current setup for Aggregation Trunking. This function allows user to add a new trunking group or modify members of an existing trunking group. When configuring the link aggregation function, users should check whether the aggregated ports are in full-duplex mode and same speed.

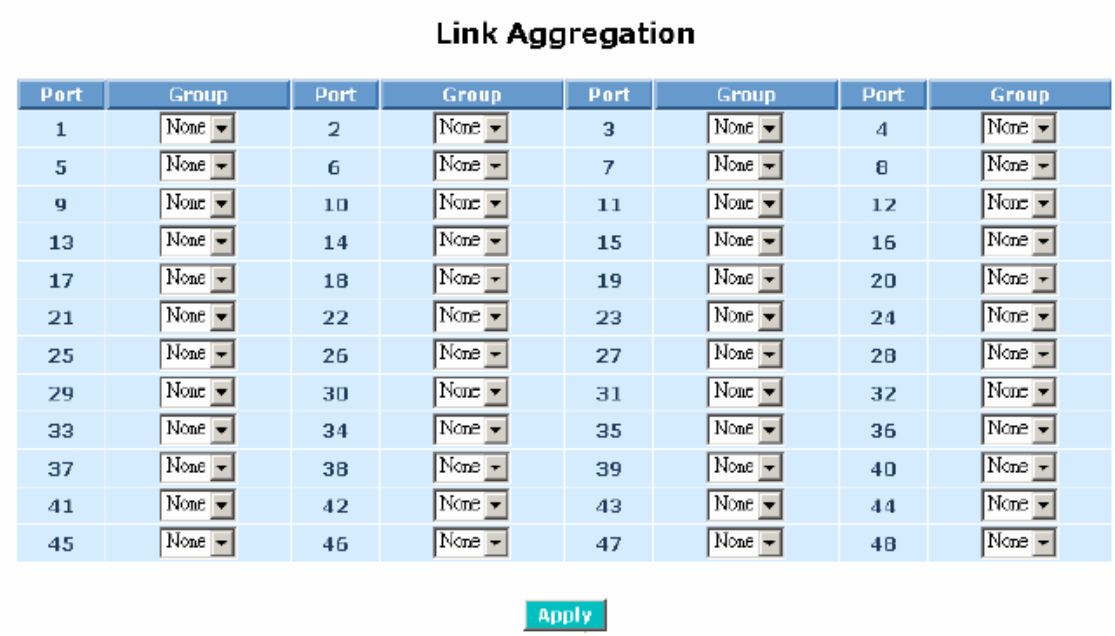

Link Aggregation
Port
Group
Port
Group
Port
Group
Port
Group
1 None 2 None 3 None 4 None
5 None 6 None 7 None 8 None
9 None 10 None 11 None 12 None
13 None 14 None 15 None 16 None
17 None 18 None 19 None 20 None
21 None 22 None 23 None 24 None
25 None 26 None 27 None 28 None
29 None 30 None 31 None 32 None
33 None 34 None 35 None 36 None
37 None 38 None 39 None 40 None
41 None 42 None 43 None 44 None
45 None 46 None 47 None 48 None
Apply

Figure 3.27 Link Aggregation

Parameter	Description
Port	Port 1~48 could be chosen as logical group of Link Aggregation.
Group	Defines the Logical Group for Link Aggregation with L1~L24 available. Maximum 8 ports per logical group. Click **<Apply>** to have the setting take effect.

3.9 Alarm Configuration

3.9.1 Trap Events Configuration

The Trap Events Configuration function is used to enable the switch to send out the trap information when pre-defined trap events occurred. The switch offers 5 different trap events for switch management. The trap information can be sent out in three ways, including email, mobile phone SMS (short message system) and trap. The message will be sent when users tick ( ) the trap event individually.

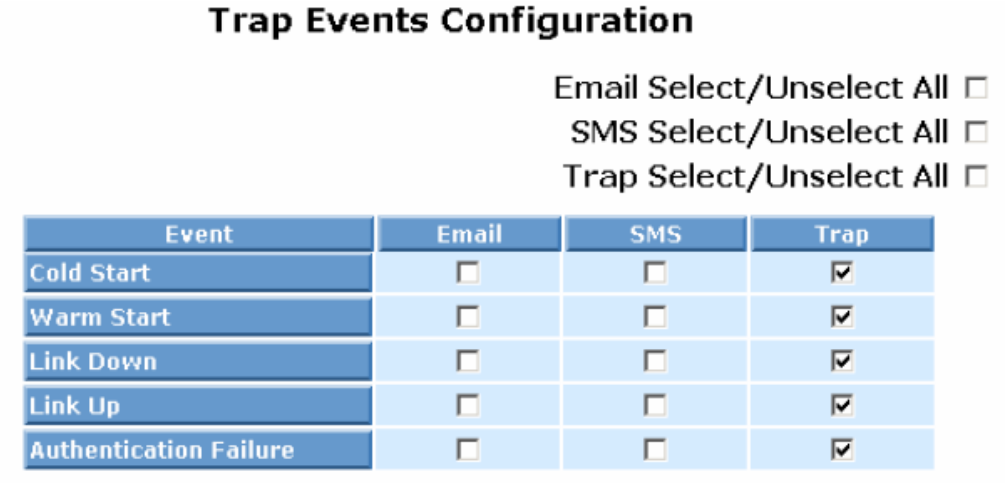


Figure 3.28 Trap Events Configuration

3.9.2 Email/SMS Configuration

Alarm configuration is used to configure the person who should receive the alarm message via email, SMS, or both. An email address or a mobile phone number has to be set in the alarm configuration. This function provides fields for 6 email addresses and 6 mobile phone numbers. The 5 different trap events will be sent to SNMP Manager when trap event occurs. After ticking trap events, users can fill in your desired email addresses and mobile phone numbers. Click **<Apply>** to have the setting take effect.

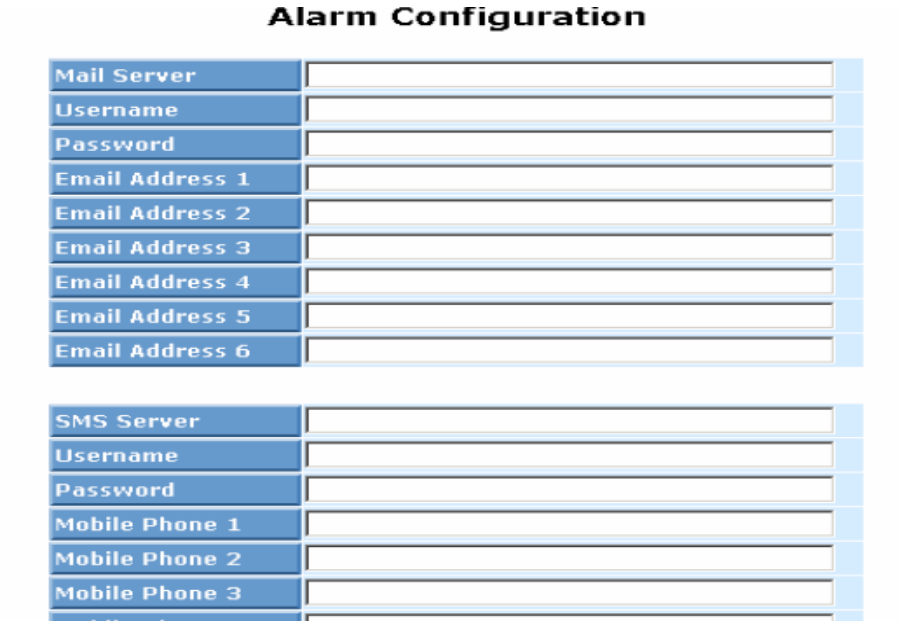


Figure 3.28 Alarm Configuration

Parameter	Description
Trap	In the switch, there are 6 trap hosts supported. Each of them has its own community name and IP address, which is user-definable. To set up a trap host, the trap manager will assign an IP address to host the trap message. In other words, the trap host is a network management unit with SNMP manager receiving the trap message from the managed switch and SNMP agent issuing the trap message. 6 trap hosts can prevent important trap messages from lost. For each public trap, the switch supports trap events include, Cold Start, Warm Start, Link Down, Link Up and Authentication Failure. When enabled, the corresponding trap will actively send a trap message to the trap host when trap event occur. If all public traps are disabled, no public trap message will be sent. Since, Enterprise (no. 6) trap is classified as private trap, which are listed in the Trap Alarm Configuration function folder. *Default: 'Enable'.*
Mail Server	IP address of the server transferring the email.
Email Username	Username on the mail server.
Email Password	Password on the mail server.
Email Address 1 – 6	Email addresses to receive the alarm message.
SMS Server	IP address of the server transferring the SMS.
SMS Username	Username in ISP.
SMS Password	Password in ISP.
Mobile Phone 1-6	Mobile phone numbers to receive the alarm message.

3.10 Configuration

The switch supports three copies of configuration, including the default configuration, working configuration and user configuration.

3.10.1 Save Start

Save the current configuration as a startup configuration file in flash memory.

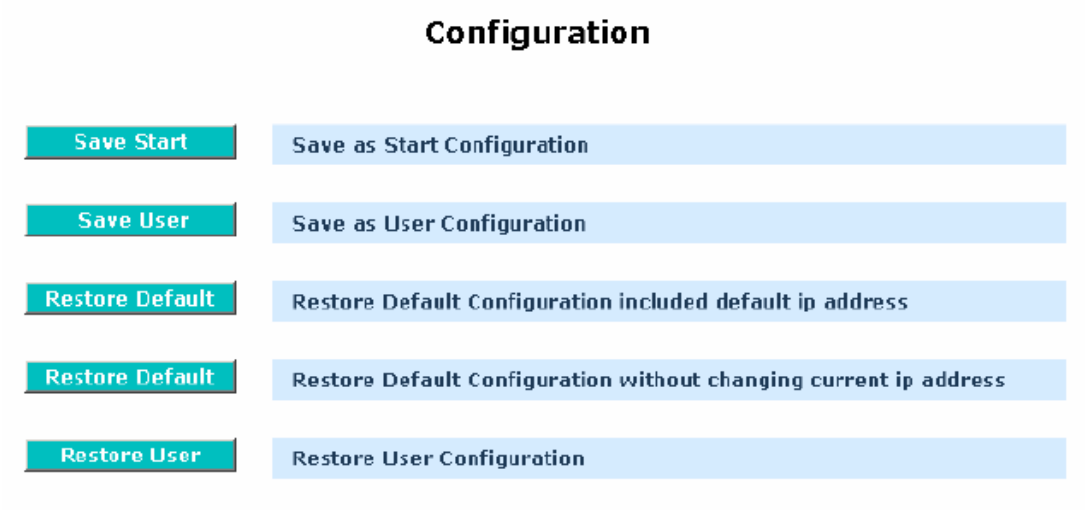


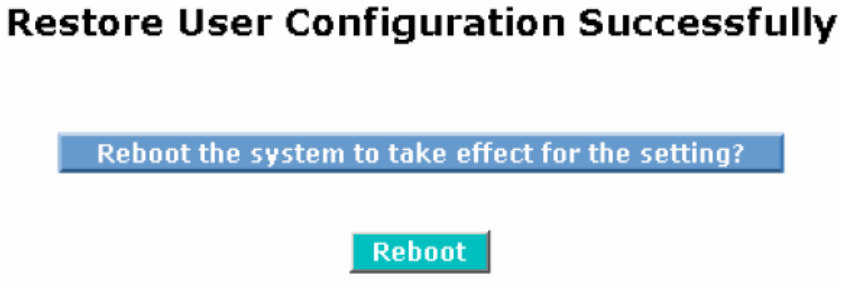
Figure 3.29 General Configuration

3.10.2 Restore Default

The function can retrieve factory setting to replace the Start Configuration. The IP address of the switch will also be restored to 192.168.1.1.

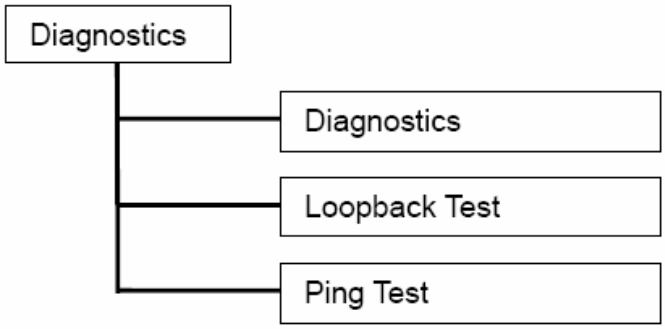
3.10.3 Restore User

This function can retrieve the previous confirmed working configuration stored in the flash memory to update the start configuration. The switch will need to be rebooted for the effect to take place.



3.11 Diagnostics

The switch includes three self-diagnostics tools: Diagnostics, Loopback Test and Ping Test.



3.11.1 Diagnostics

Diagnostics function provides a set of basic system diagnosis for determining the system health. The basic system check includes, EEPROM, UART, DRAM and Flash tests.

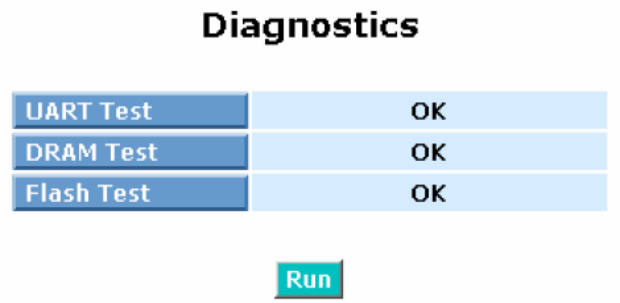
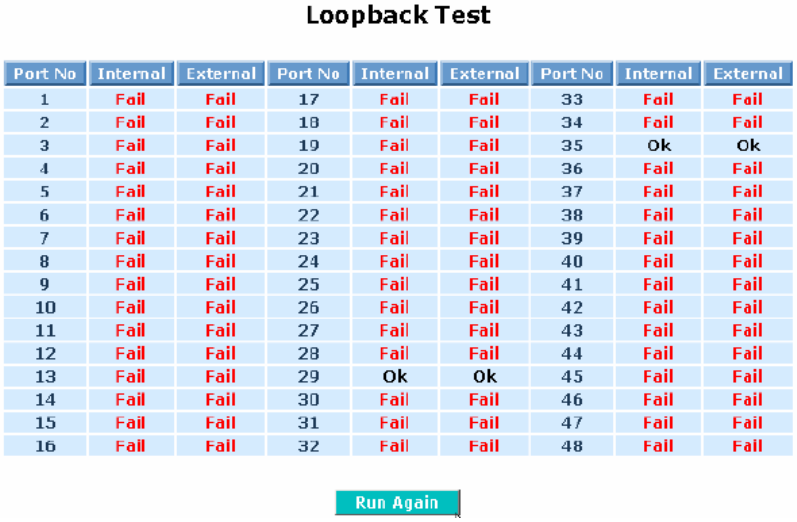


Figure 3.30 Diagnostic Results

3.11.2 Loopback Test

In the Loopback Test, there are two different loopback tests. The former test, Internal Loopback, will not send the test signal outside the switch box. The test signal only wraps around in the switch box. The second test, External Loopback, will send the test signal to its link partner. If the connection is not active between partners, the test result will indicate port link is down and report port number failed. During both tests, the system will be temporarily interrupted where all port will stop sending or receiving packets.



Port No	Internal	External	Port No	Internal	External	Port No	Internal	External
1	Fail	Fail	17	Fail	Fail	33	Fail	Fail
2	Fail	Fail	18	Fail	Fail	34	Fail	Fail
3	Fail	Fail	19	Fail	Fail	35	Ok	Ok
4	Fail	Fail	20	Fail	Fail	36	Fail	Fail
5	Fail	Fail	21	Fail	Fail	37	Fail	Fail
6	Fail	Fail	22	Fail	Fail	38	Fail	Fail
7	Fail	Fail	23	Fail	Fail	39	Fail	Fail
8	Fail	Fail	24	Fail	Fail	40	Fail	Fail
9	Fail	Fail	25	Fail	Fail	41	Fail	Fail
10	Fail	Fail	26	Fail	Fail	42	Fail	Fail
11	Fail	Fail	27	Fail	Fail	43	Fail	Fail
12	Fail	Fail	28	Fail	Fail	44	Fail	Fail
13	Fail	Fail	29	Ok	Ok	45	Fail	Fail
14	Fail	Fail	30	Fail	Fail	46	Fail	Fail
15	Fail	Fail	31	Fail	Fail	47	Fail	Fail
16	Fail	Fail	32	Fail	Fail	48	Fail	Fail

Figure 3.31 Loopback Tests

3.11.3 Ping Test

Ping Test function is a tool for detecting if the target device is active through ICMP protocol, which abounds with report messages. The switch provides Ping Test function to know if the target device is available. Simply fill in a known IP address and then click **<Ping>** button. After few seconds, the switch will report the pinged device is active or inactive in Ping Result field.

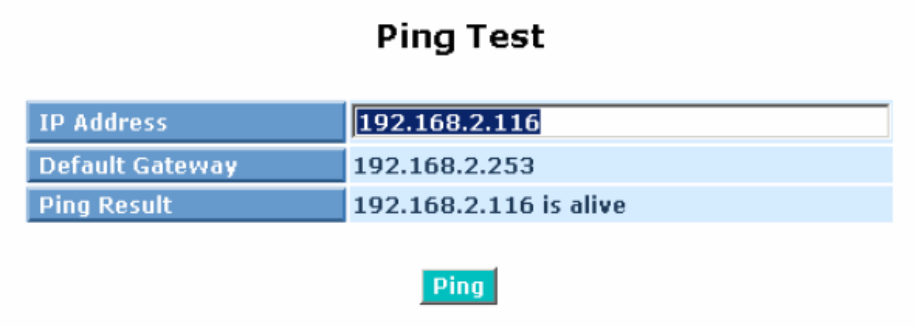


Figure 3.32 Ping Test

Parameter	Description
IP Address	An IP address in the version of v4. (E.g. 192.168.1.1)
Default Gateway	IP address of the default gateway.

3.12 TFTP

3.12.1 TFTP Server

Specify the IP address where the TFTP server is located. Fill in the IP address of TFTP server and click **<Apply>** to have the setting take effect.

Figure 3.33 TFTP Server

Parameter	Description
Server	The field for entering IP address of TFTP server.

3.13 Log

The function shows the log data provided by the switch. There are 19 private trap logs and 5 public trap logs. The switch supports total of 120 log entries. For more details on log items, please refer to the section on Alarm Configuration and SNMP Configuration.

3.13.1 Log Data

The Trap Log Data is displaying the log items including all SNMP Private Trap events, SNMP Public traps and user logs.

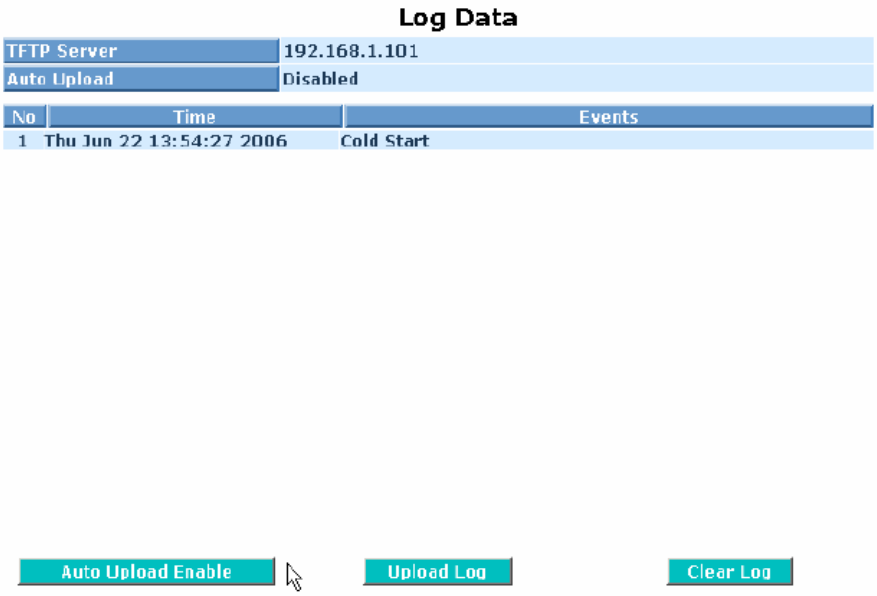


Figure 3.34 Log Data

Parameter	Description
TFTP Server	TFTP Server IP address. Log upload requires user to specify TFTP server.
Auto Upload	Auto Upload Status.
No.	Display the order number in which the trap event happened.
Time	Display the time when the trap happened.
Events	Display the trap event name.
Auto Upload Enable	Switch the enable or disable status of the auto upload function.
Upload Log	Upload log data through TFTP.
Clear Log	Clear log data.

3.14 Firmware

Firmware upgrade tool is used to help upgrade the software in order to fix or improve the function. The switch provides a TFTP client for software upgrade and can be done through Ethernet.

3.14.1 Firmware Upgrade

Follow the procedure to upgrade firmware of equipment to a newer version via TFTP client. Switch must not be powered off during the procedure and will cause unexpected damages to the equipment.

1. Specifying the IP address where TFTP server is located. The field should contain the IP address specified by the user.
2. Specifying the filename and location of the file. Users must specify full path and filename.
3. Click **<Upgrade>** button. If download is not successful, the switch will revert back to 'Firmware Upgrade' and it will not upgrade the software.
4. If the download is successful, a reboot message will be prompted and it is necessary that the switch is rebooted for settings to take effect.

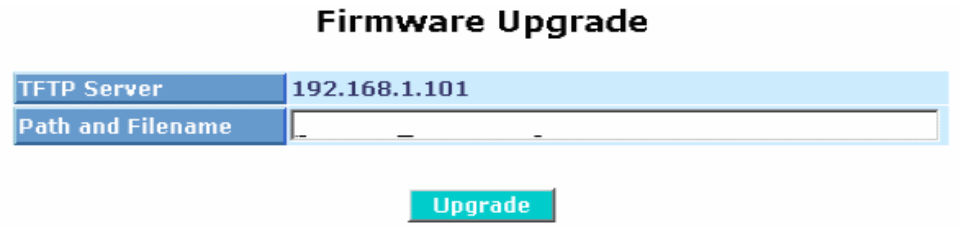


Figure 3.35 Firmware Upgrade

Parameter	Description
TFTP Server	TFTP servers for uploading the image file for upgrade.
Path and Filename	File path and filename of the image file for upgrade.

3.15 Max. Packet Length

3.15.1 Maximum Packet Length Configuration

The switch is capable of dealing with Jumbo Frames of 16k in length, which suit the transmission for a large amount of data in the network environment.

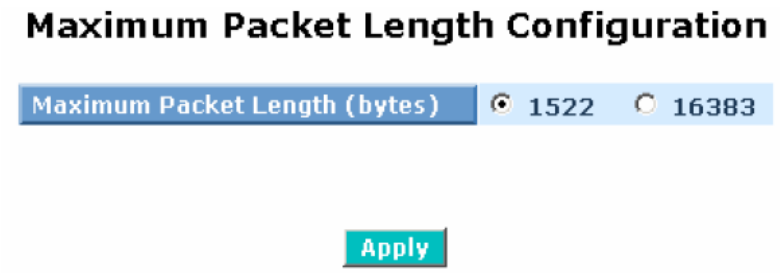


Figure 3.36 Maximum Packet Length

Parameter	Description
Maximum (bytes)	Set up the maximum length of the packet for each port. Default: 1522 Setting Range: 1~16383

3.15.2 Static Forwarding MAC

Static Forward function allows user to create the static forward table to access a specified port of the switch. Static Forward table associated with a specified port is set up by manual input of MAC address and alias name. When a MAC address is assigned to a specific port, all of the switch traffics with this MAC address could be forwarded through this port of the switch. For adding a MAC address entry in the allowed table, three parameters are needed: MAC address, associated port, and Alias. To remove MAC address, select an existing entry and click **<Delete>** button.

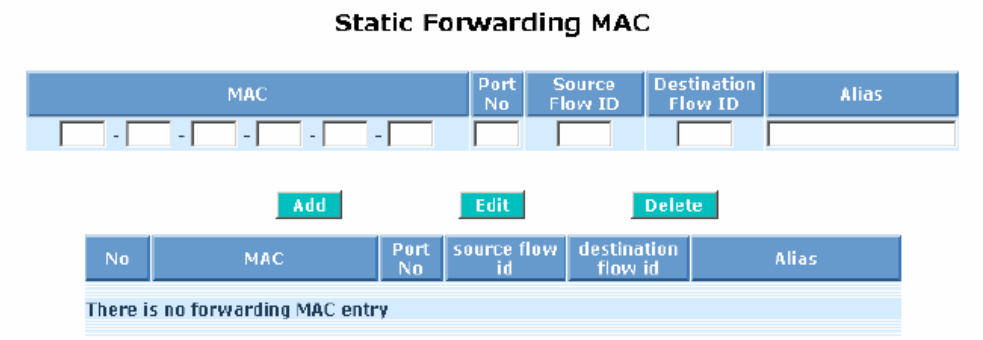


Figure 3.37 Static Forwarding MAC

Parameter	Description

MAC	It is a six-byte long Ethernet MAC address and usually expressed by hex with hyphens. (E.g. 00 – 40 - C7 - D6 – 00 – 01)
Port No	Port number of the switch. *Setting Range: 1~48.*
Source Flow ID	The parameter is influenced by Flow ID setting in QoS. *Setting Range: 0~3.*
Destination Flow ID	The parameter is influenced by Flow ID setting in QoS. *Setting Range: 0~3.*
Alias	MAC alias name assigned by users.

3.15.3 Static Filtering MAC

Static Filter function is for denying packets to forward through the switch if the packet's MAC Address is listed in the table. Users can add entries by filling in MAC address and alias then click **<Add>** button. To remove MAC address, select an existing entry and click **<Delete>** button.

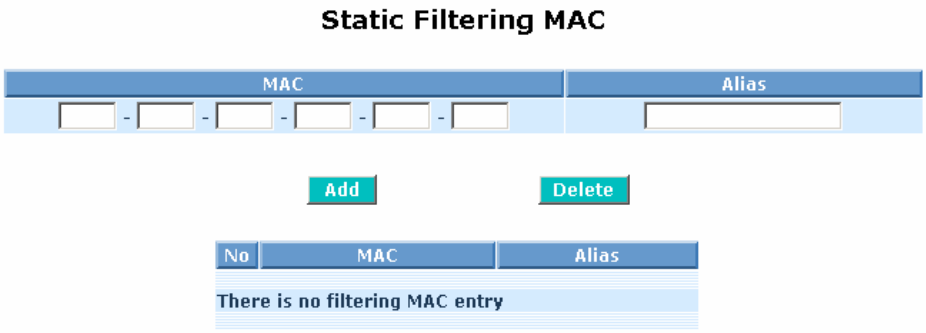


Figure 3.38 Static Filtering MAC

Parameter	Description
MAC	It is a six-byte long Ethernet MAC address and usually expressed by hex with hyphens. (E.g. 00 – 40 - C7 - D6 – 00 – 01)
Alias	MAC alias name assigned by users.

3.16 VLAN

3.16.1 VLAN Mode

The VLAN Mode Selection function includes two modes: Port-based and Tag-based. Users can specify the VLAN mode by selecting the item from the list. Click **<Apply>** to have the setting take effect.

Figure 3.40 VLAN Mode

Parameter	Description
Port-based	Port-based VLAN acts according to the port group. Packets in the same VLAN group containing list of ports can transmit data in or out. For example, a port-based VLAN named PVLAN-1 contains port 1, 2, 3 and 4. Port 1 can communicate with port 2, 3 and 4. However, port 5 cannot interact with ports in PVLAN-1. Each port-based VLAN must be assigned a group name. The switch can support up to maximum of 72 port-based VLAN groups.
Tag-based	Tag-based VLAN identifies its member by VID. If there are any rules in ingress filtering list or egress filtering list, the packet will be screened with more filtering criteria to determine if it can be forwarded. Each tag-based VLAN must be assigned VLAN name and VLAN ID. Valid VLAN ID is 1-4094 and users can create up to 256 Tag VLAN groups.

3.16.2 Tag-based VLAN

It shows the information of existing Tag-based VLAN Groups. Users can create, edit and delete a Tag-based VLAN group by pressing the associated buttons. Users can add a new VLAN group by inputting a new VLAN name and VLAN ID. In the switch, logical ports also could be created as VLAN group. Logical Ports are set according to the configuration of Link Aggregation that could create 24 sets of logical ports.

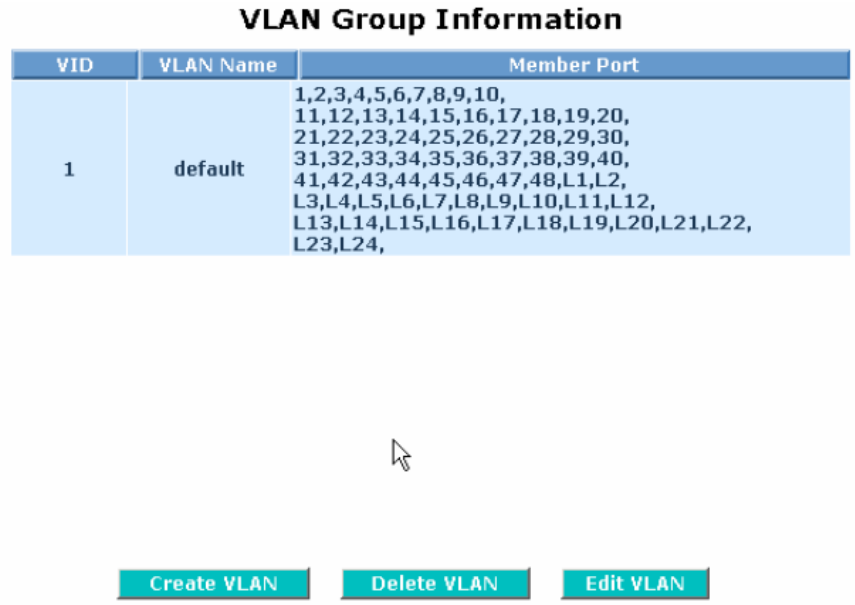


Figure 3.41 VLAN Group Information

Parameter	Description
VLAN Name	The name defined for VLAN group by administrator. Valid letters are A-Z, a-z, 0-9, " - " and "_" characters. The maximum length is 15 characters.
VLAN ID	VLAN identifier. Each tag-based VLAN group has a unique VID. It appears only in tag-based and double-tag mode.
Member Port	This is used to enable or disable a port for membership of the added VLAN. Tick the checkbox ( ) beside the port to enable it.
Create VLAN	Create a new Tag-based VLAN. Input the VLAN name and select the member by ticking the checkbox beside the port No. Click **<Apply>** to have the setting take effect.
Delete VLAN	Click **<Delete VLAN>** button to remove the selected group entry from the Tag-based group table.
Edit VLAN	Select a group entry and click **<Edit VLAN>** button to modify a group's description and member set.
All Port Unchecked	Checkbox of all member ports will become unchecked after **<All Port Unchecked>** is selected.
All Port Checked	All uncheck box of all member ports will become checked after **<All Port Checked>** is selected.

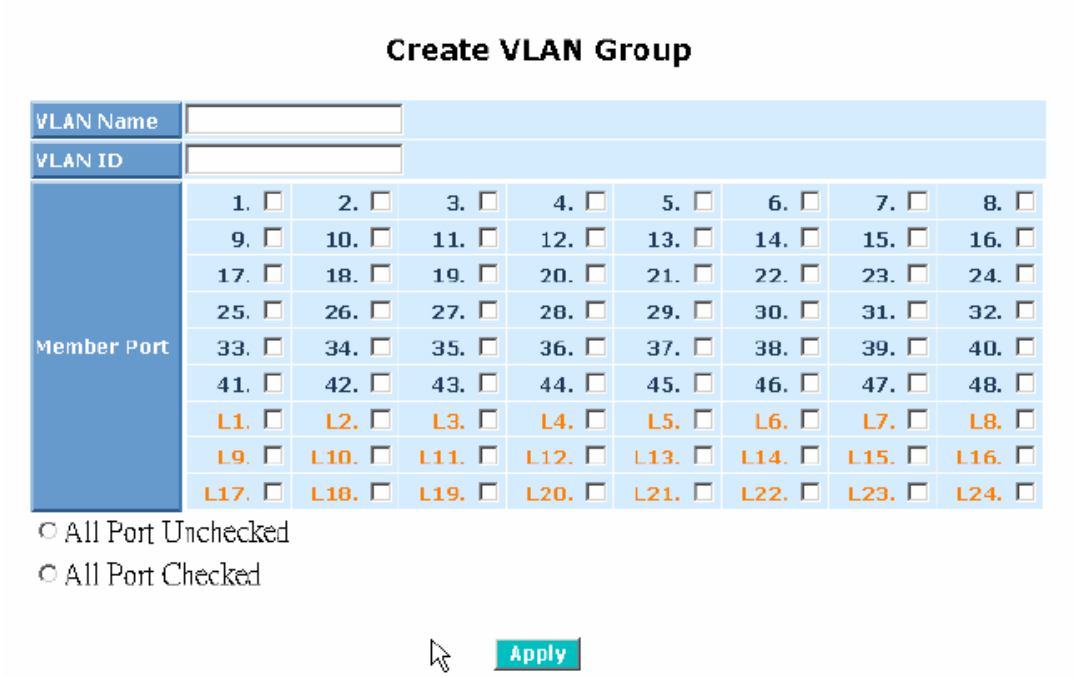
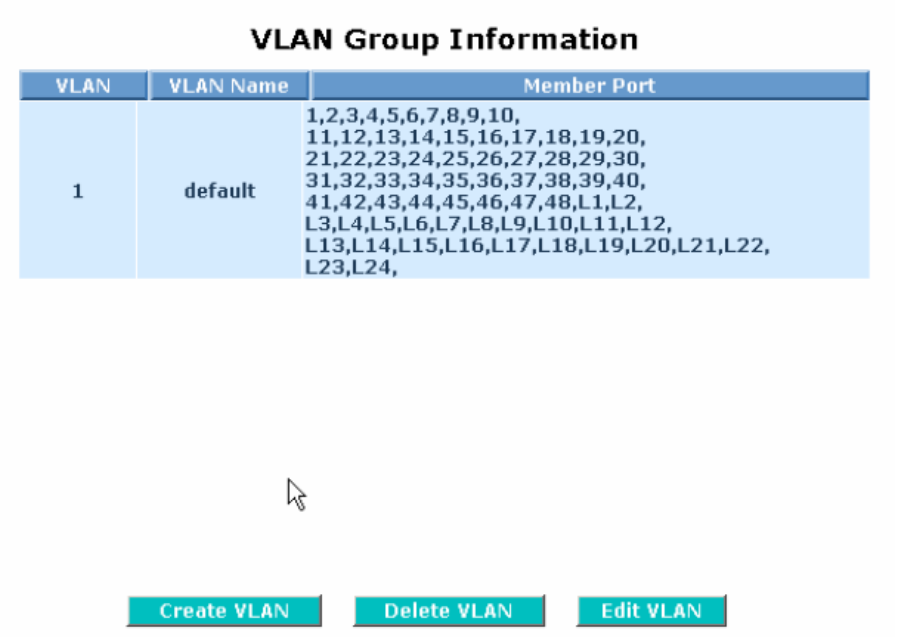


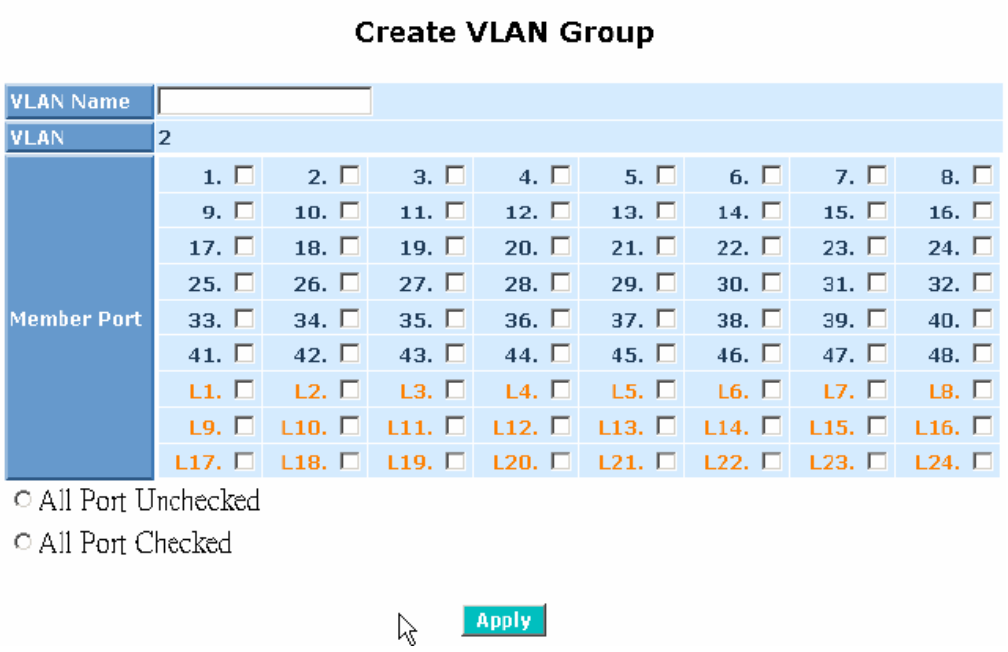
Figure 3.42 Create VLAN Group

3.16.3 Port-based VLAN

The function shows the information of the existing Port-based VLAN Groups. Users can create, edit and delete a Port-based VLAN group by pressing the associated buttons. Users can add a new VLAN group by inputting a new VLAN name. In the switch, logical ports also could be created as VLAN group. Logical Ports are set according to the configuration of Link Aggregation that could create 24 sets of logical ports.



Parameter	Description
VLAN Name	The name defined for VLAN group by administrator. Valid letters are A-Z, a-z, 0-9, " - " and "_" characters. The maximum length is 15 characters.
VLAN ID	VLAN group index.
Member Port	This is used to enable or disable a port for membership of the added VLAN. Tick the checkbox ( ) beside the port to enable it. Port-based VLAN group could include physical ports (1~48) or logical ports (1~24).
Create VLAN	Create a new Port-based VLAN. Input the VLAN name and select the member by ticking the checkbox beside the port No. Click **<Apply>** to have the setting take effect.
Delete VLAN	Click **<Delete VLAN>** button to remove the selected group entry from the Port-based group table.
Edit VLAN	Select a group entry and click **<Edit VLAN>** button to modify a group's description and member set.
All Port Unchecked	Checkbox of all member ports will become unchecked after **<All Port Unchecked>** is selected.
All Port Checked	All uncheck box of all member ports will become checked after **<All Port Checked>** is selected.



3.16.4 Port Protocol Setting

Protocol-based VLAN is based on 802.1q tag VLAN, which is classification rules based on PVID configuration. Users must apply Tagged-based VLAN in advance. The switch supports IPv4, IPv6, ARP, RARP, User Defined 0, User Defined 1 and User Defined 2. When packets belonging to ipv4 and does not contain VLAN's tag, the switch will add PVID to the packets. It will follow the rule of the configuration from VLAN Port Protocol Setting. If the packets have specific tag and VID, it will follow the rule of the configuration from VLAN tagged group.

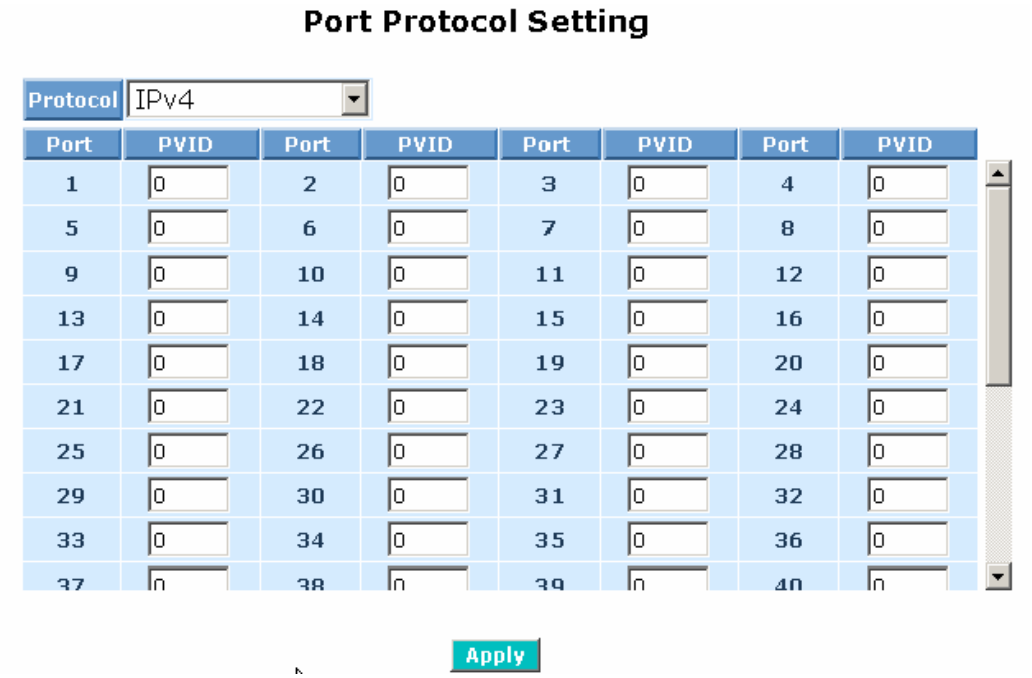


Figure 3.43 Port Protocol Setting

Parameter	Description
Protocol	Including IPv4, IPv6, ARP, RARP, User Defined 0, User Defined 1 and User Defined 2. User 0~2 would be determined in User-Defined function.
PVID	In PVID Setting, users can assign Port Permanent VLAN ID to each port. It is for untagged packets that enter the switch and operate in designated VLAN group after adding the VLAN tag according to PVID. The range of PVID number is the same as VID from 1 to 4094. Usually, before users set a number as PVID, it would create a Tag-based VLAN with VID using the same number. This is due to the fact, if port 1 receives an untagged packet, the switch will add PVID (assume VID 2) to this packet. The packet will be forwarded to VLAN group of VID 2 created by the user in advance.

3.16.5 Port VID

Port VID is applied to untagged packets entering the switch. The packet will be added a VID and forward to the VID group according to PVID number. In the switch, VLAN has different modes to use for all kinds of network environment. The switch supports four modes: Access, Private, Trunk and Hybrid. When using ‘Access’ mode, the switch only accepts untagged packets. The behavior of ‘Private’ Mode is similar to ‘Access’ mode where the only difference is that Private ports couldn’t communicate with Private ports or Access Ports. For ‘Private’ mode, it can only communicate with Trunk ports or Hybrid ports. In “Trunk” mode, the trunk ports only accept tagged packets. Trunk ports would only transmit tagged packets. In “Hybrid” mode, the trunk ports only accept tagged packets. Trunk ports would only transmit tagged packets but with an exception where VID of VLAN group for the packets is the same as PVID of the port.

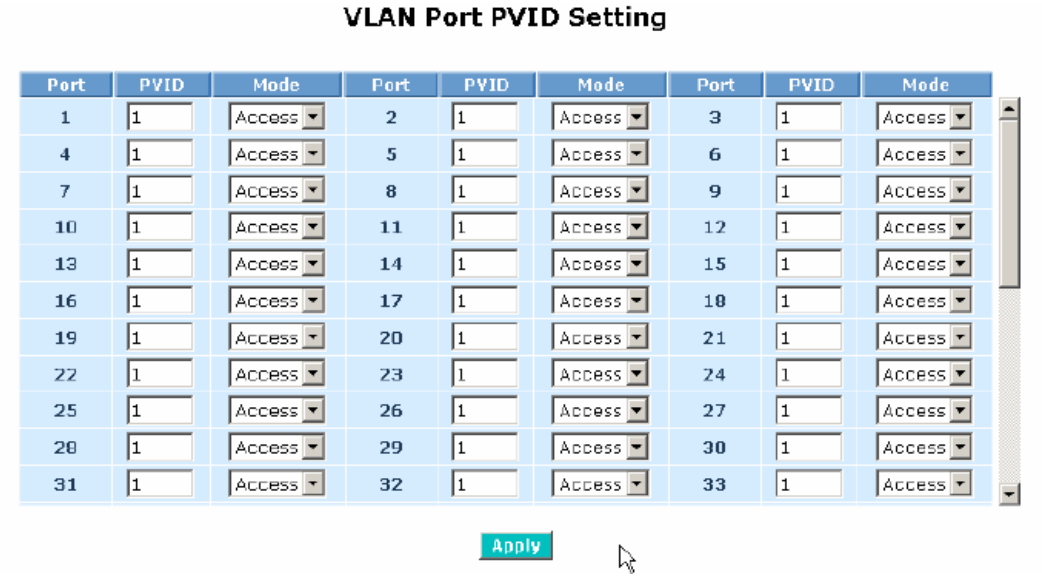

VLAN Port PVID Setting
Port PVID Mode Port PVID Mode Port PVID Mode
1 1 Access 2 1 Access 3 1 Access
4 1 Access 5 1 Access 6 1 Access
7 1 Access 8 1 Access 9 1 Access
10 1 Access 11 1 Access 12 1 Access
13 1 Access 14 1 Access 15 1 Access
16 1 Access 17 1 Access 18 1 Access
19 1 Access 20 1 Access 21 1 Access
22 1 Access 23 1 Access 24 1 Access
25 1 Access 26 1 Access 27 1 Access
28 1 Access 29 1 Access 30 1 Access
31 1 Access 32 1 Access 33 1 Access
Apply

Figure 3.44 VLAN Port PVID Setting

Parameter	Description
PVID	Before users set a number x as PVID, it is necessary to create a Tag-based VLAN with VID x. For example, if port x receives an untagged packet, the switch will apply the PVID (assume as VID y) of port x and add tag to this packet. The packet then will be forwarded as the tagged packet with VID y. *Setting Range: 1~4094.*
Mode	Modes available are ‘Access’, ‘Private’, ‘Trunk’ or ‘Hybrid’. Click **<Apply>** to have the setting take effect.

3.17 Reboot

3.17.1 Reboot the System

To reboot the system, click **<RESET>** button on the front panel of the switch. It will take around thirty seconds to complete the system boot.

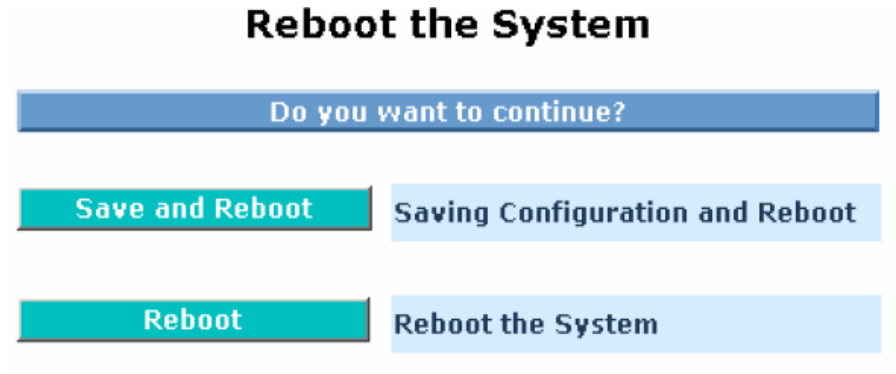


Figure 3.45 Reboot the System

Parameter	Description
Save and Reboot	Save the current settings as start configuration before rebooting the switch and system.
Reboot	Reboot the system without saving changes to the setting.

3.18 Logout

Users can manually logout in this function. Otherwise, user can set the time for auto-logout in Auto Logout function. It could prevent the network administrator from forgetting to logout from Web-based UI. Turn ‘Auto Logout’ as OFF and the users will not ever be logged out.

Figure 3.46 Logout

Parameter	Description
Logout	Click **<Logout>** button to exit the system straight away.
Auto Logout	Allow users to turn the function on or off. If no actions are detected for the set time, the switch automatically logout. *Default: ‘On’.*

4. Troubleshooting

4.1 Q&A

1. Resolving no link condition.
   The possible causes of no link condition are as follows:
   i. The attached device is not powered on.
   ii. Incorrect type or faulty cable.
   iii. The installed building premise cable is faulty.
   iv. The port may be faulty.
2. Computer A can connect to Computer B, but cannot connect to Computer C through the Gigabit Web Smart Switch.
   i. The network device of Computer C may fail to work. Please check the link/act status of Computer C on the LED indicator. Try another network device on this connection.
   ii. The network configuration of Computer C may be incorrect. Please verify the network configuration on Computer C.
3. The uplink connection function fails to operate.
   i. The connection ports on other side must be connection ports. Please check if connection ports are used on that Gigabit Web Smart Switch.
   ii. Please check the uplink setup of the Gigabit Web Smart Switch to verify the uplink function is enabled.
4. The console interface cannot appear on the console port connection.
   i. Gigabit Web Smart Switch has no console port, so users cannot use console interface to connect with Gigabit Web Smart Switch.
5. How to configure the Gigabit Web Smart Switch?
   i. User can use Web browser program in Windows environment to control the web smart functions in Gigabit Web Smart Switch. First, choose any port in Gigabit Web Smart Switch. Then, use browser and type default IP address (192.168.1.1) to connect to Gigabit with RJ45 network line. Finally, the login screen will appear immediately.

5. Technical Specification

Standards	IEEE802.3 / 802.3u / 802.3ab / 802.3z / 802.3x
Buffer Memory	768 KB on-chip frame buffer
Mac Address Table	8K entries
Interface	• 44 x Port 10/100/1000Mbps TP • 4 x Port Gigabit TP/SFP Fiber
Bridging	• Tag-based VLAN (802.1Q) • Port-based VLAN • Port Mirror, Port Sniffer • Port Trunk • Jumbo frame (16k bytes)
QoS	• QOS modes (DSCP, 802.1p and port priority) • Scheduling (Weighted Round Robin) • Multicast and broadcast storm control • 4 shaper queues • ACL QoS load
Security	• ACL rules for traffic classification and prioritize • VLAN for isolation of traffic between users.
Management	Web-based, Console, Telnet
SNMP & MIBs	SNMP, All MIB OIDs, RMON MIB
Data Transfer Rate	10M(Half duplex)/20M(Full duplex) 100M(Half duplex)/200M(Full duplex) 1000M(Full duplex)
Switch Fabric	96 Gbps
Filtering / Forwarding Rate	10Mbps: 14,880pps 100Mbps: 148,800pps 1000Mbps: 1,488,000pps
Emission	CE
Environment	Operating Temperature: 0 ^{o} - 40 ^{o} C Operating Humidity: 5% - 90%
Dimension	442(W) x 248.6(D) x 44 (H) mm
Power Supply	100-240V AC, 50-60Hz

Network Interface

Configuration	Mode	Connector	Port
10/100/1000Mbps Gigabit TP	NWay	TP (RJ-45)	1-48
1000Base-SX Gigabit Fiber	1000 FDX	*SFP	44-48
1000Base-LX Gigabit Fiber	1000 FDX	*SFP	44-48
1000Base-LX Single Fiber WDM (BiDi)	1000 FDX	*SFP	44-48

**Port 44-48 are TP/SFP fiber dual media ports with auto detected function*

**Optional SFP module supports LC or BiDi LC transceiver*

Cable and Maximum Length

Cable Type	Distance
TP	Cat. 5 UTP cable up to 100m.
1000Base-SX	Up to 220/275/500/550m, depending on Multi-Mode Fiber type.
1000Base-LX	Single-Mode Fiber up to 10/ 30/ 50km.
1000Base-LX WDM (BiDi)	Single-Mode Single Fiber up to 20km.

LED definition

LED	Status	Operation
System LED		
POWER	On/Green	Power is on
CPU	Blink/Green	Switch is working properly
	Off	CPU fails or initializes
10/100/1000Ethernet TP Port (1 to 48 port)		
LINK/ACT	On/Green	Link with remote device is good
	Blink/Green	Traffic is present
	Off	Link is off or bad connection
10/100/1000M	On/Green	1000M link is detected
	Blink/Green	100M link is detected
	Off	10M or no link is detected
1000SX/LX Gigabit Fiber Port (44 - 48 port)		
SFP (LINK/ACT)	On/Green	Link with remote device is good
	Blink/Green	Traffic is present
	Off	Link is off or bad connection

- **Transmission Mode:** 10/100Mbps supports full/half duplex and 1000Mbps supports full duplex only.
- **Transmission Speed:** 10/100/1000Mbps for TP and 1000Mbps for Fiber.
- **MAC Address and Self-learning:** 8K MAC address and 256 VLAN table entries.
- **Flow Control:** IEEE802.3x is compliant for full duplex and backpressure flow control is for half duplex.